И. Н. Кузнецов

БИЗНЕС-БЕЗОПАСНОСТЬ

И. Н. Кузнецов

БИЗНЕС-БЕЗОПАСНОСТЬ

6-е издание

Москва
Издательско-торговая корпорация «Дашков и К°»
2021

УДК 65.012
ББК 65.290
К89

Рецензенты:
С. К. Купрейчик, кандидат юридических наук, доцент;
Е. А. Тихоненко, кандидат экономических наук, профессор.

Кузнецов И. Н.

К89 Бизнес-безопасность / И. Н. Кузнецов. — 6-е изд. — М.: Издательско-торговая корпорация «Дашков и К°», 2021. — 412 с.

ISBN 978-5-394-04382-6

Представленное издание оригинально по своей структуре и содержанию, так как включает теорию, методику и практические рекомендации по обеспечению личной и общественной безопасности.

В книге рассматриваются практические вопросы обеспечения экономической безопасности организации: функционирование служб безопасности, защита коммерческой тайны, информационных ресурсов, обеспечение безопасности внешней деятельности, личной безопасности руководителей и персонала, в том числе и в зарубежных поездках.

Советы и практические рекомендации помогут избежать многих неприятностей и неожиданностей, которыми сегодня полна наша неспокойная жизнь, разобраться в сложившихся трудных ситуациях и принять правильное решение.

Для руководителей и сотрудников организаций всех форм собственности и хозяйствования, банковских и финансовых учреждений, правоохранительных органов и охранных служб, а также для учащихся, студентов, изучающих курс «Основы безопасности жизнедеятельности», и тех, кто интересуется проблемами самозащиты и выживания.

ISBN 978-5-394-04382-6

Оглавление

ВВЕДЕНИЕ

Основные задачи предлагаемой читателю книги — раскрыть содержание и важнейшие направления безопасности фирмы, ее руководителя, а также помочь в создании специальной службы, осуществляющей реализацию всех защитных мероприятий в условиях новых экономических отношений.

Любой из нас сегодня желает стабильности в работе и повседневной жизни. Каждый руководитель отвечает за обеспечение стабильной деятельности своего объекта — офиса, банка, магазина. Стабильная работа возможна при надежной защите от различных угроз, убытки от которых могут быть неисчислимы. Есть угрозы здоровью и даже жизни сотрудников и посетителей объекта, материальным ценностям, оборудованию, коммерческой и личной тайне.

Оценить угрозы и методы защиты от них в каждом конкретном случае можно путем привлечения специализированных фирм и создания соответствующих структур, обеспечивающих защиту предпринимательства.

Успех в мире бизнеса в значительной мере зависит от правильности и обоснованности выбранной стратегии предпринимательской деятельности. При этом должны учитываться вероятности критических ситуаций.

Для любого бизнеса важно не избежание риска вообще, а его предвидение и снижение до минимального уровня. Чтобы успешно вести дело, недостаточно быть предприимчивым, инициативным, рисковым, — прежде всего необходимо знать правила и нормы, которые регулируют поведение людей в сложных условиях рыночной экономики.

Эта книга — своего рода практическое пособие, которое поможет предпринимателю в яростной конкурентной борьбе обеспечить основные виды защиты, а для этого определить: что

искать, где искать, чего остерегаться, что делать, как это делать.

Часть вопросов, рассматриваемых в книге, заинтересует более широкий круг читателей, которые в той или иной мере нуждаются в защите от насилия в нашем непредсказуемом обществе.

При подготовке этого пособия использовалась литература и статьи различных авторов, которые более или менее подробно старались раскрыть отдельные вопросы безопасности и методы защиты фирмы, ее руководителя.

В последнее время в России повышается спрос на товар "безопасность", причем на товар разного уровня и качества. Государственная система безопасности не успевает реагировать на стремительно растущие потребности рынка.

Переход к рыночной экономике — это, по сути дела, движение в сферу повышенного риска, и здесь во всей остроте встает новая для нас, но известная в мировой практике проблема экономической безопасности фирм.

Получение субъектами хозяйствования самостоятельности предполагает и ответственность за результаты деятельности, безопасность которой приобретает особое значение в связи с ростом преступности, и особенно организованной, активизацией зарубежной экономической разведки и промышленного шпионажа, повсеместным применением жестких мер воздействия на руководителей фирм, предпринимательские структуры.

Отсутствие у ряда юридических и физических лиц навыков принятия оптимальных управленческих решений для устойчивой работы в условиях рыночных отношений, малая осведомленность о процедурах и правилах обеспечения экономической безопасности делают их уязвимыми перед экономическими преступлениями, правонарушениями и противоправными действиями "партнеров".

Экономическая безопасность — это такое состояние производственных отношений и организации информационно-правовых связей, материальных, финансовых и интеллектуальных ресурсов, при котором гарантируются стабильность функцио-

нирования, финансово-коммерческий успех, прогрессивное использование научно-технических достижений и социальное развитие субъектов хозяйствования.

Она обеспечивается системой мер, осуществляемых государственными органами, администрацией фирм и специально создаваемыми службами безопасности, а также частными охранными агентствами.

В предлагаемой книге рассматриваются основные вопросы экономической безопасности фирмы: создание службы безопасности, организация режима и охраны, обеспечение безопасности внешней и хозяйственно-финансовой деятельности, характеризуются все этапы защиты коммерческой тайны как важной составной части системы экономической безопасности. Значительное место отведено организации обеспечения безопасности деятельности банков и финансовых компаний, роли персонала фирм в обеспечении защиты конфиденциальной информации.

В настоящее время происходит все более интенсивное насыщение фирм и финансовых учреждений компьютерной и телекоммуникационной техникой, бурное развитие которой, как свидетельствует мировой опыт, сопровождается ростом правонарушений, связанных с кражами, злоупотреблением и несанкционированным доступом к данным, хранящимся в памяти компьютеров и передаваемым по линиям связи. По этой причине встает во весь рост проблема надежного обеспечения безопасности информационных ресурсов как одной из важных составляющих экономической безопасности субъектов хозяйствования.

Однако соответствующих разработок, рекомендаций, пособий, методик, обобщающих возможные противоправные действия конкурентов, преступных организаций и отдельных лиц и дающих на основе этого возможность субъектам хозяйствования предпринять упреждающие действия по защите своей экономической безопасности, имеется недостаточно.

Устранению в определенной мере этого пробела послужат материалы предлагаемой книги, в основу которой положен оте-

чественный и зарубежный опыт теоретических исследований и практических материалов в области обеспечения экономической безопасности с учетом современных тенденций развития информационных технологий и их приложений в сфере предпринимательской деятельности.

Существенный интерес представляют специальные разделы *по мерам личной безопасности предпринимателя и обеспечению* безопасности загранпоездок.

Книга будет полезна для руководителей предприятий, фирм, банков, финансовых компаний, охранных фирм и агентств и других организаций, а также для всех интересующихся вопросами предпринимательства и бизнеса, студентов вузов, учащихся средних специальных учебных заведений, слушателей факультетов переподготовки и повышения квалификации.

1. ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ ФИРМЫ

1.1. Организация режима и охраны

1.1.1. Основные задачи организации режима и охраны

Режим и охрана — это сочетание организационных, регламентационных и контрольных мер, направленных на обеспечение полной (круглосуточной, в течение длительного времени), частичной (только в ночное или дневное время) или выборочной (при завозе ценных грузов, на определенный отрезок времени и т. п.) сохранности физических лиц, материальных и финансовых ценностей, зданий и помещений фирмы, а также любых сведений о деятельности фирмы, не подлежащих разглашению. Соблюдение этих мер обязательно для всех сотрудников, посетителей и клиентов.

Руководители и сотрудники фирмы, обеспечивающие и осуществляющие режим и охрану, руководствуются в своей деятельности соответствующим законодательством, нормативными документами и методическими рекомендациями.

Цель создания и поддержания режима и охраны определяет их задачи, выбор способов, а также сил и средств для охраны.

Задачи режима и охраны подразделяются на основные и обеспечивающие.

К ***основным задачам*** относятся:

- обеспечение сохранности зданий и помещений фирмы;
- обеспечение сохранности и контроль за перемещением материальных ценностей;

• обеспечение пропускного режима (или контроль за допуском граждан в здания и помещения);

• обеспечение сохранности собственной информации о деятельности фирмы;

• поддержание противопожарной безопасности.

В число ***обеспечивающих задач*** входят:

• подбор, подготовка и расстановка сил и средств охраны;

• контроль функционирования системы режима и охраны;

• материально-техническое обеспечение режима и охраны;

• сбор и анализ информации о состоянии режима.

Наиболее эффективным представляется сочетание возможностей, предоставляемых государством, частными агентствами и службами безопасности фирм.

1.1.2. Организация пропускного режима

Пропускные документы. Обычно устанавливаются следующие виды пропускных документов, дающих право прохода сотрудников и посетителей в фирму, вноса (выноса), ввоза (вывоза) материальных ценностей:

1) удостоверения;

2) пропуска.

Пропуска могут быть постоянными, временными и разовыми — для сотрудников и посетителей, а также материальными — для ввоза (вывоза) материальных ценностей.

В **удостоверении** в обязательном порядке должна быть фотография, заверенная печатью, указаны должность, дата его выдачи и срок действия. Руководителем фирмы может быть утвержден перечень удостоверений, выданных другими организациями, по которым разрешен допуск в фирму.

На удостоверениях и пропусках проставляются печати, предусмотренные правилами режима, и цифровые знаки, определяющие зону доступности, период их действия, право проноса портфелей (кейсов, папок и др.). Период пребывания сотрудников в фирме в рабочее и нерабочее время определяется руководством с проставлением цифрового знака на удостоверении или пропуске.

Образцы удостоверений и пропусков разрабатываются службой безопасности и утверждаются руководством.

Утвержденные образцы удостоверений личности, пропусков, оттисков цифровых знаков, печатей (штампов), проставляемых на удостоверениях и пропусках, списки с образцами подписей руководителей или уполномоченных лиц, имеющих право подписывать удостоверения и пропуска, передаются начальнику отдела режима и охраны под расписку.

Полная замена удостоверений и постоянных пропусков осуществляется, как правило, через 3–5 лет. Через 2–3 года производится их перерегистрация с проставлением соответствующей отметки.

Для перерегистрации, замены или изменения пропускных документов ежегодно по состоянию на 1 января в службу безопасности представляются отделом кадров списки сотрудников с указанием должности, фамилии, имени, отчества и наименование документа с соответствующими пометками "круглосуточно", "рабочее время с ... по ...", "с портфелем", в какую зону и т. п.).

Удостоверения и постоянные пропуска могут выдаваться лицам, не работающим в фирме, по отдельному утвержденному руководством списку с указанием учреждения, должности, фамилии, имени, отчества и сопроводительных пометок. Эти документы должны постоянно храниться в бюро пропусков (или у уполномоченного лица) и выдаваться посетителям в момент прибытия. После завершения работы эти лица сдают документы в бюро пропусков.

Удостоверения и постоянные пропуска выдаются указанным лицам на основании письменных ходатайств руководителей учреждений, где они состоят в штате.

Временные пропуска с фотографиями на срок до трех месяцев выдаются лицам, работающим временно или прикомандированным. Временные пропуска без фотографии на срок до одного месяца действуют при предъявлении паспорта (удостоверения личности). Продление действия временных пропусков допускается на срок не более двух месяцев.

Разовый пропуск действителен в течение 30 минут с момента выдачи до входа в здание, а также в течение 15 минут после отметки о времени ухода посетителя из фирмы.

Руководитель подразделения, в котором находится посетитель, обязан на обороте разового пропуска сделать отметку о времени ухода посетителя и расписаться с указанием полностью своей фамилии.

Удостоверения или постоянные пропуска выдаются сотрудникам при поступлении на работу на основании приказа о зачислении в штат.

Учет пропускных документов. Учет бланков удостоверений и пропусков, их оформление и выдача осуществляются бюро пропусков.

Использованные постоянные и временные пропуска уничтожаются по мере необходимости, но не реже одного раза в год.

Для учета документов по пропускному режиму ведутся следующие учетно-контрольные документы:

- дело с приказами и распоряжениями по пропускному режиму;
- дело с заявками структурных подразделений на удостоверения, постоянные и временные пропуска;
- дело с инструкциями по пропускному режиму и образцами подписей на материальные пропуска;
- дело с актами на уничтожение пропускных документов;
- дело переписки по пропускному режиму;
- книга учета ежедневного расхода бланков разовых пропусков;
- книга учета выдачи удостоверений, постоянных и временных пропусков.

Кроме того, бюро пропусков ведет книгу учета посетителей по разовым пропускам.

Печати и штампы. Для оформления всех видов пропусков в бюро пропусков должны быть следующие печати и штампы:

- круглая (диаметр 25 мм) или треугольная каучуковая печать для разовых и материальных пропусков;

• круглая рельефная металлическая или каучуковая печать для удостоверений и постоянных пропусков (диаметр 20 мм);

• штампы цифровых знаков;

• штампы "ПОГАШЕН", "ОБРАЗЕЦ", "ВРЕМЕННЫЙ".

В журнале учета печатей и штампов предприятия против оттиска каждого штампа или печати делается описание его содержания и назначения.

При замене печатей и штампов на новые старые уничтожаются, о чем составляется акт, а в журнале делается соответствующая запись. На новые заводятся новые графы.

1.1.3. Обеспечение охраны стационарных объектов

В содержательном плане обеспечение безопасности стационарных объектов представляет собой многогранный процесс реализации охранных мероприятий, по большей части предупреждающего характера. Действительно, эффективной может считаться лишь такая система охраны, которая либо просто не позволяет злоумышленникам найти лазейку в режиме безопасности, либо создает возможность пресечения преступных посягательств на самой ранней стадии.

В основе разработки системы защиты объекта и обеспечения ее функционирования лежит принцип создания последовательных рубежей безопасности, на которых угроза должна быть своевременно обнаружена, а ее распространению будут препятствовать надежные преграды.

Такие рубежи должны располагаться последовательно, от забора вокруг территории объекта до главного, особо важного помещения, такого, как хранилище ценностей и коммерческой тайны.

В качестве примера рассмотрим защиту от несанкционированного проникновения.

Злоумышленник проникает на территорию объекта, на которой располагаются здания и стоянки автомашин посетителей и сотрудников. Возможная угроза для территории — кража автомобилей, их порча или установка взрывных или подслу-

шивающих устройств. Защита территории должна состоять из различного рода ограждений ее периметра и специально оборудованных въездов и проходов, охранной сигнализации, охранного освещения и охранного телевизионного наблюдения.

Но злоумышленник может не остановиться и попытаться проникнуть дальше, в здание и затем в хранилище ценностей и информации. Отсюда ясно, что средства защиты всех участков объекта должны взаимно дополнять друг друга и эффективность всей системы защиты от несанкционированного проникновения будет оцениваться как минимальное время (несколько десятков минут), которое злоумышленник затратит на преодоление всех рубежей безопасности. За это время должна сработать охранная сигнализация, сотрудники охраны должны установить причину тревоги, принять меры к задержанию злоумышленника.

Таким образом, эффективность системы защиты оценивается в зависимости от времени, прошедшего с момента возникновения угрозы до начала ее ликвидации. Чем более сложная и разветвленная система защиты, тем больше времени требуется на ее преодоление и тем больше вероятность того, что угроза будет обнаружена, определена, отражена и ликвидирована.

К числу факторов, влияющих на выбор приемов и средств охраны, относятся:

- возможные способы преступных посягательств на охраняемый объект;
- характеристика технической укрепленности охраняемого объекта;
- наличие и характеристики средств охранно-пожарной сигнализации;
- наличие уязвимых мест в технической укрепленности объекта, которые известны только охране и службе безопасности;
- условия местности, на которой расположен охраняемый объект, а также его конструктивные особенности;
- режим и характер работы охраняемого объекта, его технологические характеристики, имеющиеся на объекте материальные и финансовые ценности;

• режим охраны объекта;

• количественные и качественные характеристики сил охраны;

• вооруженность и техническая оснащенность охранников, наличие у них автотранспорта, средств связи, сигнализации и специальных средств.

Режим охраны объекта по времени может иметь круглосуточный, частичный (определенные часы суток) или выборочный характер.

В зависимости от количества используемых сил и средств, плотности контроля территории и объекта режим охраны может быть простым или усиленным.

На значительной части охраняемых объектов охранники присутствуют круглосуточно. В дневное время контролируют посетителей, прибывающих на объект, осуществляют контрольно-пропускной режим, а в ночное время обеспечивают закрытую охрану объекта, принимая на себя полную ответственность за его сохранность.

Некоторые объекты охраняются лишь эпизодически, т. е. выборочно по времени. К таким объектам относятся квартиры, охраняемые на период отсутствия хозяина, временные хранилища или территории — на период завоза товарно-материальных ценностей и др.

Существует несколько видов охраны, в частности:

1) охрана с помощью технических средств с подключением на пульт централизованного наблюдения с установкой автоматической сигнализации;

2) охрана путем выставления постов (силами отдела охраны или силами полиции);

3) комбинированная охрана.

Охрана с помощью технических средств. Для охраны и контроля состояния помещений на объекте охраны широко используются различные по назначению и техническому исполнению средства охраны. С их помощью можно обнаружить возникновение пожара, проникновение постороннего лица через периметр помещения, просто нарушение периметра, например,

если ветром распахнет окно или будет разбито стекло в окне, перемещение кого-либо или чего-либо внутри помещения, прикосновение к контролируемому предмету, например, сейфу, находящемуся внутри помещения.

Как правило, для охраны помещений, проникновение в которые посторонних лиц нежелательно, используется комплекс технических средств, реализующих многорубежную защиту помещений.

Применение многорубежной защиты существенно повышает надежность охраны, так как появляется страховка на случай, если один из рубежей не сработает из-за неисправности или каких-то преднамеренных действий злоумышленника, возможно, знакомого с современными системами охранной сигнализации.

Первым рубежом защищаются строительные конструкции периметров помещений, оконные и дверные проемы, люки, вентиляционные каналы, тепловые вводы, тонкостенные перегородки и другие элементы помещений, доступные для проникновения с внешней стороны, в том числе и те из них, которые оборудованы стальными решетками.

Вторым рубежом с помощью специальных приборов охранной сигнализации защищаются помещения внутри здания.

Третий рубеж перекрывает охраняемые хранилища внутри помещений, средства и материальные ценности и др.

Интересным является использование многоуровневых компьютерных систем контроля пропускного режима на проходных предприятия, контроля доступа в здания и помещения.

Их функциональные возможности позволяют осуществлять следующие режимы доступа:

- по электронному пропуску;
- по электронному пропуску и PIN-коду;
- блокировку входа;
- свободный проход;
- программирование доступа по времени (по дням недели для сотрудников, на сутки для посетителей, программирование выходных дней и праздников).

Системой отображаются события в режиме реального времени на планах охраняемого объекта со всеми точками контроля доступа и расположения датчиков.

Обеспечивается получение следующих справок:

• об аварийных ситуациях на объекте, в данном помещении с указанием времени, даты и типа события;

• по сотруднику, с указанием времени, даты и помещений, в которые он заходил в текущие сутки, неделю;

• по помещению, с указанием перечня сотрудников, даты и времени посещения данного помещения.

Обеспечивается учет рабочего времени при выходе из строя рабочей станции или пропадании питающего напряжения.

Охрана путем выставления постов. Охрана с подключением помещений предприятия на пульт централизованной охраны не всегда представляется возможной. В таких случаях рекомендуется организовать постовую охрану.

Посты могут выставляться и для усиления уже имеющейся охраны. Наличие постов значительно снижает возможность преступных посягательств на собственность фирмы как в ночное, так и в дневное время. Особенно эффективен этот вид охраны в случаях попыток преступников остаться в помещениях предприятия после окончания рабочего дня.

Комбинированная охрана. И охрана путем выставления постов, и охрана с помощью технических средств имеют свои сильные и слабые стороны. Вторая обладает рядом несомненных преимуществ по сравнению с постовой охраной. Это и одновременный контроль за большим количеством помещений при минимальном участии человека, и непрерывная работа в течение длительного времени.

В то же время она уступает постовой охране в том, что в полной мере может использоваться только в нерабочие часы охраняемого объекта. Разумное сочетание этих двух видов охраны позволяет с максимальной надежностью защитить помещения от нежелательных посещений как в рабочее, так и в нерабочее время. Особенно эффективна комбинированная охрана, если ее объектом является многоэтажное или любое другое здание с множеством помещений.

Режим охраны. Эффективный режим охраны призван обеспечить сохранность зданий и помещений на объекте, сохранность и контроль за перемещением материальных ценностей и людей, предупредить утечку информации о деятельности объекта, поддерживать противопожарную безопасность. Решающее значение для режима охраны имеют квалифицированный подбор, подготовка и расстановка сил и средств охраны, сбор и анализ информации о состоянии режима охраны, а также контроль функционирования службы безопасности на объекте.

В практике деятельности подразделений охраны по обеспечению безопасности выделяются две группы задач режима охраны объекта:

1) аналитические и предупредительные;

2) процедурно-отражательные.

Аналитические задачи решаются путем систематического сбора информации о субъектах преступной деятельности и состоянии собственного режима охраны. Главным здесь является соблюдение принципов непрерывности и постоянства сбора информации.

Решение *предупредительных задач* связано, в первую очередь, с созданием имиджа сильного и надежного режима охраны. Подобный имидж может быть создан серией имитационных мероприятий, демонстрирующих "неудачные" попытки посягательства на объект и мощное противодействие охраны преступникам. Все это может быть дополнено впечатляющей демонстрацией элементов режима охраны (внушительного вида охранники, современная охранная сигнализация, присутствие полиции на объекте и т. д.).

Предупредить покушение на охраняемый объект можно также путем его маскировки, перекрытия информационных каналов о его деятельности и дезинформации конкурентов и криминальных элементов о характере деятельности, форме собственности, состоянии режима охраны, объеме имеющихся на объекте товарно-материальных ценностей и т. д.

Процедурно-отражательные задачи режима охраны объекта решаются путем своевременного обнаружения признаков готовящегося посягательства с последующим его отражением предварительно подготовленными силами и средствами.

Как правило, подобное мероприятие (операцию) следует проводить во взаимодействии с сотрудниками органов внутренних дел, которые будут иметь возможность своевременно зафиксировать следы преступной деятельности.

В тех случаях, когда время начала посягательства трудно предугадать, имеет смысл в отдельных случаях "подтолкнуть" преступников к началу посягательства. Это может быть достигнуто путем дезинформирования криминальных элементов о времени и месте ввоза ценных грузов, крупной суммы денег и т. п.

При организации охраны объекта служба безопасности должна предусмотреть в перечне служебных обязанностей охранников варианты их действий на случай возникновения на объекте или поблизости от него различного рода критических ситуаций.

В таких случаях обязанностью охранника является:

- принятие мер к задержанию преступника и сопровождение задержанного в орган внутренних дел;
- обеспечение охраны места происшествия, находящихся на нем следов и вещественных доказательств до прибытия сотрудников полиции;
- оказание помощи пострадавшим от преступления или несчастного случая до прибытия медицинских работников;
- установление свидетелей и очевидцев происшествия, в том числе и для того, чтобы обеспечить самому себе оправдательную свидетельскую базу;
- сообщение в орган внутренних дел о фактах нарушения общественного порядка поблизости от объекта.

Особое внимание деятельности охранников следует уделять при решении задач обеспечения проведения на охраняемом объекте деловых встреч и приемов партнеров по бизнесу.

В этом плане служба охраны должна обеспечить:

- встречу гостей, прибывающих на деловой прием;

• согласование действий основной охраны и телохранителей приглашенных лиц;

• охрану одежды, вещей гостей и их автомашин на прилегающей территории;

• предупреждение инцидентов между гостями на деловом приеме или встрече;

• контроль состояния напитков, закусок и других угощений, приготовленных для гостей;

• выявление участников мероприятия, которые дольше обычного задерживаются возле стола, ведут себя необычно;

• наблюдение за лицами:

— приходящими на деловую встречу или прием со свертками, портфелями, кейсами и т. п.;

— приносящими на мероприятие аудио- или видеоаппаратуру;

— которые пришли и очень быстро покинули место встречи;

• выявление в зале приемов и смежных помещениях предметов, которые могут быть источником опасности для гостей;

• проведение мероприятий против прослушивания разговоров организаторов и гостей в помещениях и по телефону.

1.2. Посягательства на собственность фирмы и основы организации противодействия им

Многие граждане серьезно озабочены ростом преступности в стране. Особую тревогу у предпринимателей и бизнесменов вызывают объединение преступников в организованные группы, повышение уровня их вооруженности и технической оснащенности, сращивание этих групп с коррумпированными должностными лицами, увеличение числа убийств, дерзких видов вымогательств, хищений, взяточничества и других преступлений.

Объектом посягательства со стороны преступных группировок часто становится имущество фирмы, собственность, находящаяся в ее помещениях. Поэтому состояние и надежность охраны зданий

и помещений фирмы, состояние режима охраны, как правило, определяют цели, задачи, характер сил, средств и методов самого посягательства, а также условия (оперативную обстановку), в которых происходит посягательство и его отражение.

Вид и методы конкретного посягательства зависят от частных целей, преследуемых преступной группировкой в каждом конкретном случае. Условно их можно разделить на три группы.

Во-первых, преступные, т. е. уголовно наказуемые, посягательства.

Из них наиболее характерными могут быть:

— предъявление требований передачи здания и помещений фирмы или права на пользование ими под угрозой насилия, шантажа или причинения вреда;

— вымогательство под угрозой убийства, причинения тяжких телесных повреждений или повреждения здания и помещений фирмы;

— вымогательство, повлекшее причинение крупного ущерба зданию и помещениям фирмы;

— умышленное уничтожение или повреждение здания и помещений фирмы, совершенное путем поджога или иным общеопасным способом, а также повлекшее человеческие жертвы или повлекшее тяжкие последствия.

Во-вторых, посягательства не преступные, но могущие причинить различного рода ущерб зданию и помещениям фирмы:

— использование, вопреки воле и желанию законного владельца, здания и помещений фирмы в своих целях, не имеющих противоправного характера;

— использование в тех же целях сотрудников фирмы во время их пребывания в здании и помещениях.

В-третьих, это может быть комбинированное сочетание как преступных, так и непреступных видов и методов посягательств на здание и помещения фирмы в зависимости от конкретных целей.

Так, если перед преступниками стоит цель разового завладения материальными ценностями, например, путем мошенничества, кражи, грабежа или разбоя, то решение этой задачи будет связано с разведкой, изучением системы охраны, выяснением вида возможного противодействия и его интенсивности, наличием путей отхода и т. п.

Если же речь идет о вымогательстве (рэкете), причем не однократном, а относительно постоянном (дань), то задачи будут стоять совершенно иные. Помимо вышеперечисленных, это, прежде всего, блокирование возможного обращения в правоохранительные органы или к иным адресатам за помощью путем угроз, принятие предупредительных мер на случай, если угроза не сработает, или же предложение со стороны преступной группировки услуг по обеспечению режима безопасности от посягательств со стороны себе подобных. Такой "налог" за "охрану" может составлять 10–20% доходов фирмы.

К сожалению, граждане не защищены законом от навязывания подобного рода услуг путем угроз, шантажа, компрометации, запугивания.

Вымогательство в отношении лиц, работающих в сфере легального бизнеса (предприниматели, кооператоры, индивидуальная трудовая деятельность), осуществляется путем реальной угрозы жизни, здоровью, имуществу и т. п.

В сфере нелегального бизнеса вымогательство осуществляется преимущественно путем угрозы и шантажа разоблачением противоправной деятельности перед правоохранительными органами. При этом не исключаются как физическая расправа, так и повреждение имущества, например, путем поджога.

В зависимости от целей изменяется количественный и качественный состав сил и средств посягательства.

К непосредственному посягательству причастны, как правило, представители низшей ступени в иерархии организованной преступности. Так называемая элита и технические исполнители организуют, направляют, определяют: первая — стратегическую, а вто-

рые — тактическую линию поведения. Они причастны только к выработке общих задач и определению общих целей посягательств.

Характерно, что в руководстве любой преступной группировки присутствуют постоянное соперничество, скрытая или явная вражда по многим вопросам преступного бизнеса, закамуфлированная общностью целей и путей их достижения.

Деятельность лидеров организованной преступности строится на следующих ***основных принципах***:

• они не принимают никакого участия в непосредственном совершении преступлений, не общаются с другими членами преступных группировок, избегая всего, что может их скомпрометировать;

• общее руководство они осуществляют через своего особо проверенного и доверенного представителя;

• вопросы наказания провинившихся "коллег" они решают сообща и реализуют через посредников;

• вопросы бизнеса также решаются на уровне элиты и реализуются через доверенных лиц.

Непосредственные исполнители посягательства — это, прежде всего, пестрый конгломерат расхитителей, воров, спекулянтов, мошенников и т. д. — лица, постоянно живущие на нетрудовые доходы. Рядовые члены преступной группы, как правило, подчиняются строгой дисциплине и выполняют определенные функции — разведчики, боевики, охранники. На две последние должности привлекаются физически подготовленные молодые люди (обычно бывшие спортсмены).

Методы действия подобных групп отличаются исключительной наглостью, жестокостью, цинизмом, неразборчивостью в выборе средств.

Как показывает практика, к уголовной ответственности за совершение конкретных преступлений привлекаются в основном рядовые исполнители, а их руководители и идейные вдохновители для закона недосягаемы.

Подготовка и техническое оснащение преступных групп также зависят от целей посягательства. Для обеспечения своей безопасности они стремятся установить контакты с представи-

телями правоохранительных органов, во многих случаях небезуспешно. Этим объясняется утечка информации из органов правопорядка и как следствие — успешное применение контрмер со стороны организованной преступности.

Техническая оснащенность некоторых преступных групп может вызвать зависть. Они располагают самой совершенной импортной аппаратурой, видеотехникой, радиосвязью, портативными компьютерами, имеют новейшие, с мощными моторами, автомашины, вооружены стрелковым армейским нарезным оружием, гранатами, минами, используют документы прикрытия и средства маскировки.

Выбор преступной группой методов посягательства на здание и помещения фирмы зависит и от возможных способов противодействия, т. е. от состояния режима охраны.

В настоящее время с различной степенью уверенности в успехе можно рассчитывать на помощь в деле охраны со стороны следующих государственных органов, негосударственных организаций и частных лиц.

В системе Федеральной службы войск национальной гвардии РФ кроме различных оперативных и специальных подразделений, существует служба "Охрана" (ФГУП "Охрана" Росгвардии), с которой можно заключить договор на охрану зданий и помещений.

Органы ФСБ России также могут защитить законные права и интересы граждан, но только в тех случаях, когда речь идет о посягательстве на интересы государственной безопасности.

В принципе, можно обратиться непосредственно в прокуратуру или суд, но они не имеют своих специальных сил и средств для защиты интересов граждан и в соответствии с законом привлекут для этого подразделения МВД и ФСБ России.

Все вышеперечисленные структуры как правоохранительные органы объединяет то, что они, как правило, реагируют на посягательство, обладающее двумя признаками. Во-первых, речь должна идти об общественно опасных действиях, предусмотренных уголовным законодательством, и, во-вторых, посягательство должно создавать угрозу или быть реальным. Если же вред не причинен

или нет реальной угрозы его причинения, то, по закону, правоохранительные органы охраняют здание и помещения фирмы наравне с иными объектами охраны.

То обстоятельство, что правоохранительные и другие государственные органы оказались не готовыми к эффективной борьбе с организованной преступностью, а их кадровое, материально-техническое обеспечение и координация их деятельности не соответствуют современным требованиям, послужило одним из оснований для возникновения различного рода негосударственных охранных организаций.

Кроме государственных правоохранительных органов и негосударственных организаций, охрану здания и помещений фирм могут осуществлять и частные лица на договорной или иной основе.

В идеальном варианте охрану должны осуществлять профессионалы органов МВД и ФСБ России, которые и существуют за счет и для защиты налогоплательщиков. Жизнь, к сожалению, диктует иные условия. И хотя услуги детективных фирм не менее эффективны, поскольку там тоже часто работают те же профессионалы, стоить они будут несколько дороже.

И последнее, от чего зависит выбор преступной группировкой вида и методов посягательства, — это условия (оперативная обстановка).

В целом эти условия можно разделить на общие — характерные для страны, региона, и частные — характерные для конкретного посягательства на собственность.

Общие условия — кризисные явления в экономике, острый дефицит товаров и услуг, нарушение работы транспорта, сложности в социальной жизни, ослабление всех видов ответственности, несовершенство законодательства и его применения, конфликтные и кризисные ситуации в различных регионах страны, рост преступности и т. п.

Частные условия — численность и расстановка сил и средств в нужный момент, наличие информации у обеих сторон друг о друге, степень ее достоверности и полноты.

В целом, говоря о посягательствах на собственность фирмы со стороны преступных группировок, необходимо иметь в виду следующее.

Прежде всего, посягательство осуществляется организованными группами, имеющими строгую иерархию. Участники таких групп связаны особыми нормами поведения и строгими санкциями (наказаниями) за их нарушение.

Деятельность этих групп носит хорошо законспирированный, устойчивый характер. Каждое посягательство детально планируется и технически обеспечивается.

Реализация преступных замыслов характеризуется быстротой, решительностью, наглостью, цинизмом и жестокостью.

Особое место в посягательствах на собственность занимают вопросы "разведки" и "контрразведки". При этом во главу угла ставятся вопросы обеспечения собственной безопасности. В ход пускается весь арсенал средств — от подкупа и шантажа нужных лиц до их физического устранения. Не исключается внедрение "своих" людей в государственный аппарат и другие структуры общества.

Наличие у преступных групп больших денежных сумм и иных ценностей позволяет им материально обеспечивать свои операции. Деньги идут на дачу взяток, оплату "услуг" общеуголовных преступников, поддержание "пострадавших" (привлеченных к уголовной ответственности) и их близких.

Таким образом, идет процесс самовоспроизводства организованной преступности, пополнения новыми исполнителями, недостатка в которых, к сожалению, пока нет. Порядок набора, например, в рэкетиры довольно прост. Чаще достаточно одной рекомендации авторитетного в этой среде человека. Не удивительно, что на фоне общего числа преступлений, совершенных в стране, организованная преступность занимает существенное место.

По своему характеру посягательства на здания, помещения и другое имущество фирмы со стороны представителей организованной преступности подразделяются на конспиративные и открытые.

Такое "разнообразие" определяется различными условиями, в которых они протекают, целями, на достижение которых они направлены, специальными силами и средствами, с помощью которых они осуществляются.

Особо следует остановиться на конспиративном образе действий, к которому прибегают преступные группировки при посягательствах на здание, помещения и другое имущество фирмы.

Преступники уже давно поняли, что успех и продолжительность их "бизнеса" зависят от того, насколько скрытно и основательно будут готовиться и проводиться преступные акции как по отношению к правоохранительным органам, так и по отношению к будущим пострадавшим и окружению вообще. Поэтому соответствующая работа в этом направлении ведется ими постоянно и, как правило, на должном уровне.

Основной источник специальных знаний в этой области и необходимой информации — коррумпированные и бывшие сотрудники правоохранительных органов, участвующие в деятельности преступных группировок.

Кроме того, в преступном мире накоплен и передается из поколения в поколение определенный криминальный опыт, носителями и хранителями которого являются прежде всего "воры в законе", а также ряд других категорий преступников.

И, наконец, лица, отвечающие за вопросы конспирации в деятельности организованной преступности, пополняют свои знания, используя зарубежный опыт своих "коллег", например, путем просмотра видеофильмов, изучения соответствующей литературы (недостатка в которой за рубежом нет) и т. д.

Очевидно, что преступные элементы объединяются для совершения не единичных, а многочисленных преступлений, что требует определенной организации, управления и получения соответствующей информации. В различных группах эта работа ведется, естественно, на различном уровне профессионализма, что не исключает использования характерных методов обеспечения скрытности своей деятельности вообще и при посягательствах на здание и помещения фирмы в частности.

В их арсенале известные человечеству с незапамятных времен и отшлифованные веками методы использования лиц, добывающих информацию, конспиративных квартир, тайников, легенд прикрытия, средств маскировки и современной техники.

Рассмотрим более подробно эти довольно специфические методы.

Использование лиц, добывающих или обеспечивающих необходимой информацией преступную группу. Классифицировать этих "сотрудников" довольно затруднительно. Их многочисленный отряд включает осведомителей, агентов, шпиков, доверенных лиц, информаторов, порученцев, стукачей и т. д. Не исключается их объединение в единую сеть. При этом они, как правило, не знают друг друга.

Возможно также *внедрение* в фирму своих людей. Это трудоемкий процесс. К тому же он занимает определенное время.

Фирмы, заботясь о подборе своих сотрудников, как правило, предъявляют к ним определенные требования. Однако объективная необходимость, потребность как в специалистах, так и в техническом персонале не исключает случаев приема на работу лиц, связанных с преступным миром.

Внедрение осуществляется двумя путями. Первый — "свой человек" выступает под своей фамилией и устраивается в фирму по своей специальности.

Второй путь — внедрение под прикрытием легенды. Легенда создается специально для того, чтобы облегчить агенту завоевание доверия тех лиц, в среду которых он должен внедриться, чтобы проникнуть в нужное структурное подразделение или помещение фирмы, а также чтобы его обезопасить. При проведении подобного рода операции требуется фальшивый паспорт с ложными идентификационными данными.

Этот прием довольно эффективен, так как в последующем дает шанс лицу, внедренному в штат фирмы, уйти от ответственности. Сложность же заключается в добыче фальшивых документов и поддержании легенды. Зато в случае удачи агент получает возможность войти в курс многих дел фирмы, влиять на ход событий, детально

изучить расположение помещений фирмы и тем самым значительно облегчить процесс посягательства.

Внедрить своего человека в фирму сложно, но зато, в отличие от человека, просто снабжающего информацией преступную группу, он более надежен и легче управляем.

Подобные "услуги" по понятным причинам носят секретный характер, поскольку обе стороны — преступная группа и агент — не заинтересованы в разглашении сотрудничества.

Привлечение к сотрудничеству, другими словами — *вербовка* — может осуществляться путем запугивания, шантажа, подкупа или при добровольном согласии лица оказать услуги организованной преступности (например, из мести конкурентам). Продолжительность сотрудничества зависит от целей и задач преступной группы. Это может быть как разовое привлечение, так и длительное сотрудничество.

В зависимости от категории агента, его ценности строятся и отношения между сторонами. Очевидно, что общение с высокопоставленным, информированным и влиятельным лицом будет проводиться предельно конспиративно. Поэтому встречи могут назначаться крайне редко, в специально подобранных местах и под усиленной охраной, внешне носить бытовой характер. Получаемая информация в дальнейшем будет использоваться анонимно, без ссылки и огласки.

Не исключается соблюдение мер предосторожности и со стороны лица, работающего на организованную преступность. Информация от него может идти анонимно, через подставных лиц, не имеющих отношения к преступной деятельности (в практике отмечались случаи привлечения для этих целей детей и подростков), по телефону, телеграфу, почте и т. д.

Особое, да и, наверное, самое уязвимое для обеих сторон место занимает использование тайников для обмена информацией, материальными предметами, например, деньгами за работу.

Организация связи через тайник требует проявления особого искусства и находчивости. Известно, что этим видом связи с

переменным успехом пользуются как государственные преступники, так и законопослушные граждане (обмен любовными посланиями и т. п.).

В организацию тайника входят подбор места, изготовление хранилища для вложения передаваемых вещей, разработка операции по использованию тайника.

Место должно быть легкодоступным для обеих сторон. В зависимости от продолжительности хранения содержимого тайник может специально оборудоваться и камуфлироваться.

В операцию по использованию тайника входят помещение передаваемого в тайник, извещение об этом адресата, извлечение последним вложения и сообщение об этом первой стороне. Сам момент изъятия вложения может незаметно контролироваться организатором тайника, для того чтобы исключить случайное вмешательство в этот процесс посторонних лиц. Сигналом о вложении и об изъятии может служить так называемая метка в виде условного знака в условном месте.

Для обеспечения секретности общения не исключено проведение встреч в многолюдных местах — крупных магазинах, на рынке, вокзале, стадионе и т. п. Встреча обычно носит быстротечный характер и почти не привлекает внимания.

Общение с "менее ценными" агентами может носить обычный характер. При этом стороны особо не заботятся о своей безопасности и часто попадают в поле зрения не только правоохранительных органов, но и своих конкурентов.

Как правило, для контактов с лицами, снабжающими преступную группу информацией или оказывающими иную помощь, выделяются подготовленные члены группы, поскольку эта работа сопряжена во многих случаях с риском провала.

Не исключается и ведение своего рода картотек и иных материалов, фиксирующих подобную деятельность, например, съемка момента встречи и передачи информации коррумпированным чиновником лицу с сомнительной репутацией. В последующем такой материал может быть использован для шантажа и угроз.

Размер материального вознаграждения за оказание услуги зависит от содержания информации, трудностей ее добывания и т. п. Деньги могут передаваться по почте, телеграфу или иным (в зависимости от ситуации) способом.

Многие действия, связанные с подготовкой и проведением преступных посягательств, из соображений скрытности проводятся, как правило, на так называемых ***конспиративных квартирах***.

Цели приобретения и использования этих квартир: проведение встреч, факт и содержание которых должны оставаться в тайне; содержание похищенных заложников, предметов и ценностей; укрывательство членов преступной группы и других лиц, представляющих для преступников интерес.

Под конспиративные квартиры используют дачи, индивидуальные дома, государственный и иной жилой фонд. Они могут принадлежать подставным лицам, сниматься за высокую плату кем-то из членов преступной группы или через посредников. Часто для этих целей используются квартиры лиц, отбывших уголовное наказание и пользующихся доверием в преступной среде, реже — собственные квартиры членов преступной группы, так как это связано с большим риском.

К конспиративным квартирам обычно предъявляются следующие требования. Режим их использования и "репутация" не должны вызывать повышенного интереса как у правоохранительных органов, так и у соседей. Желательно, чтобы они имели как минимум два выхода и были расположены в удобном и не вызывающем интереса у назойливых соседей месте.

Посещение конспиративных квартир требует повышенной осторожности, чтобы исключить привлечение к ним внимания не только посторонних, но в первую очередь (в случаях слежки) — конкурентов, правоохранительных органов или негосударственных сыскных служб, поскольку "расшифровка" конспиративной квартиры в последующем поможет выйти на других членов преступной группы и даже в некоторой степени контролировать ее деятельность.

Очень близко к использованию конспиративных квартир примыкает создание представителями организованной преступности различного рода ***фиктивных фирм*** на подставных лиц.

Фирмы эти могут использоваться в тех же целях, что и конспиративные квартиры. Этот способ имеет свои преимущества. Прежде всего, статус предприятия дает возможность любым гражданам, не опасаясь и не вызывая подозрения, посещать фирму. Правда, это преимущество нередко оборачивается недостатком, ведь в числе посетителей могут оказаться лица, "визит" которых для фиктивной фирмы и ее истинных хозяев крайне нежелателен.

Значительно затрудняет борьбу с организованной преступностью использование преступниками для сокрытия своей деятельности различного рода ***легенд прикрытия***.

Преступники могут "выступать" в роли работников милиции, прокуратуры, органов госбезопасности, применяя при этом соответствующую экипировку и документы. В настоящее время, к сожалению, без труда можно приобрести форменную одежду, а с помощью множительной техники изготовить необходимое удостоверение.

Нельзя не учитывать и того, что в составе группы непосредственных исполнителей могут находиться бывшие работники этих органов, чье поведение не будет отличаться от поведения их недавних коллег.

Кроме перечисленных, с успехом используются легенды "скорой помощи", пожарной охраны, сантехнической, газовой, водопроводной и других служб. Выбор легенды практически не ограничен и зависит от возможностей, места применения и изобретательности преступников.

Применительно же к проблеме защиты здания и помещений фирмы от преступных посягательств легендирование необходимо членам преступной группы для ознакомления с обстановкой на месте предполагаемого проникновения. Поэтому истинная цель посещения всегда будет скрыта от хозяев, а взамен предложена специально подготовленная, что, по мнению преступников, не должно

насторожить лиц, с которыми им придется общаться в здании и помещениях фирмы.

Кроме того, убедив хозяев в том, что они имеют дело, например, с сотрудником правоохранительных органов, преступники от имени этих органов могут получить необходимую информацию, документы и т. д.

Если это будет "пожарник" — он сможет беспрепятственно (что входит в обязанности пожарной охраны) осмотреть все здание и помещения фирмы. Различного рода "слесари" и "сантехники", производя "профилактический осмотр", могут не только исследовать нужные им помещения, но и установить в них подслушивающие устройства.

Перечень подобного рода легенд можно продолжить. Но и без того очевидно, что выбор легенды всегда зависит от цели посягательства, а основная ее задача — за вымышленным лицом скрыть истинные намерения и не вызвать тревоги у хозяев.

Этим же целям и для поддержания разработанной легенды служат такие средства маскировки деятельности преступных групп, как использование похищенных автомашин, фальшивых номерных знаков и документов.

Кроме того, подготовка и проведение посягательства могут разделяться на части и совершаться разными преступными группами, не связанными между собой. Так, одна группа может заниматься поиском будущей жертвы и, выбрав подходящий объект, передавать сведения другой группе, которая подготовит и осуществит посягательство. Дальше, если речь идет, например, о краже, начинает действовать третья группа, реализующая похищенное.

Более солидные преступные группировки налаживают "дело" с размахом, постоянно, по их терминологии, "пасут" (контролируют) многие солидные совместные предприятия и кооперативы.

Так, в настоящее время в среде организованной преступности одним из самых доходных считаются контроль и последующее вымогательство, жертвами которого становятся предприятия, занимающиеся торговлей компьютерами и другой элек-

тронной техникой. Преступников привлекают не только многомиллионные доходы, но и возможность через эти фирмы впоследствии выйти на мировую арену.

Многочисленные случаи хищения компьютерной техники из зданий и помещений фирм говорят о том, что это действуют незначительные преступные группировки, как правило, не входящие в состав организованной преступности.

Но если деятельность фирмы отслеживается и до деталей становится известной вымогателям, то можно с уверенностью делать вывод — действует организованная преступность, так как подобного рода деятельность неорганизованным группам просто не под силу.

Некоторые группы могут специализироваться на совершении отдельных преступлений по заказу других групп или отдельных лиц. Тем самым создается своего рода рынок криминальных услуг, перечень которых довольно велик.

Например, по заказу жертвами могут стать владельцы кафе и ресторанов, которые не сговорились с представителями организованной преступности. Акты прямого насилия в отношении владельца такого заведения или членов его семьи сопровождаются организацией различных инцидентов. Ломая оборудование и мебель в кафе или провоцируя там драки, преступники отпугивают посетителей, снижают посещаемость, что также наносит заметный ущерб владельцу заведения.

Попытки шантажировать намеченную жертву могут повторяться. При этом требуемая преступниками сумма, как правило, постепенно увеличивается. К сожалению, существует и определенная такса (не астрономическая) на услуги по убийству "на заказ".

Значительно облегчает, увеличивает мобильность и динамичность совершения преступлений использование организованной преступностью ***технических средств***.

Современный уровень развития техники позволяет преступникам с помощью различного рода устройств (например, специальных микрофонов) прослушивать конфиденциальные разговоры, в том числе в здании и помещениях фирмы.

Для внедрения техники подслушивания разрабатываются целые операции с предварительным изучением места установки подслушивающих устройств, планированием и координацией действий всех участников операции.

В настоящее время хорошо организованные преступные структуры без труда приобретают подобного рода технику, специально для этих целей разработанную за рубежом. Не исключена и возможность прослушивания телефонных переговоров, причем техническое решение проблемы довольно просто.

Кроме того, преступники, используя подкуп, угрозы и шантаж, могут привлекать к этой работе сотрудников телефонной связи.

Особое место в арсенале организованной преступности занимает ***организация и ведение слежки*** за будущими жертвами.

Перед началом слежки объект наблюдения тщательно изучается:

- устанавливаются и проверяются данные о личности объекта;
- изучаются его привычки, наклонности, по возможности — образ жизни;
- детально изучается внешность наблюдаемого, особые приметы (по возможности добывается или изготавливается его фотография);
- изучается распорядок дня (рабочее время, перерывы, места отдыха);
- выясняются сведения о его семейном положении (количество членов семьи, их анкетные данные, места работы, учебы);
- устанавливаются адреса постоянного и временного жительства наблюдаемого;
- по возможности изучается место его работы, выявляются контакты с сослуживцами, характер этих контактов;
- выясняется, есть ли у объекта автомашина или иное средство передвижения (их регистрационные номера, место стоянки);
- выясняются иные вопросы — в зависимости от целей слежки.

После изучения личности и данных об объекте наблюдения продумывается и готовится сама слежка. В зависимости от образа жизни, места проживания, характера объекта и технических возможностей преступной группировки определяется, какая и какими силами будет вестись слежка.

Подобные наблюдения различаются по виду, длительности, интенсивности и целям. Кроме того, наблюдение может быть одноразовым, выборочным, периодическим, длительным и т. д.

Определившись с целями и задачами и выбрав необходимую форму, разрабатывают стратегию слежки и ее приемы.

Неподвижное наблюдение служит для контроля за определенной местностью, зданиями, предметами или лицами, не находящимися в движении. Этот прием более всего подходит для наблюдения за зданиями и помещениями фирмы.

При неподвижном наблюдении возможна съемка видеокамерой или фотоаппаратурой всего, что происходит вокруг фирмы (движущиеся люди, автомашины и т. д.). При этом не исключается попадание в поле зрения посторонних людей, вещей и событий, что, однако, не снижает эффективности данного приема, если, конечно, получаемая информация подвергается тщательному анализу.

Неподвижное наблюдение может осуществляться как одним человеком, так и группой — поочередно или всеми одновременно. Располагаются наблюдающие по возможности в таких точках, где их длительное пребывание на одном месте не вызывает подозрений. Это могут быть остановки городского и иного транспорта, кафе, рестораны, магазины и т. д.

Применяется и несколько иное расположение наблюдающих в случаях, когда отсутствие подходящего "прикрытия" исключает длительное пребывание одного и того же лица на одном месте. В этом случае помогает периодическая смена наблюдателей, которые находятся поблизости, но вне видимости объекта слежки.

Следующий прием слежки — *подвижное наблюдение.* Оно подразделяется на пешее и наблюдение с использованием транспортных средств.

Практически для того, чтобы обеспечить скрытность и продолжительность слежки, достаточно от трех до пяти наблюдателей. Слежка ведется с таким расчетом, чтобы в непосредственной близости от объекта наблюдения всегда находился лишь один наблюдающий. Помимо слежки, он обязан вести всех остальных за собой. При этом особенно важна постоянная информация о происходящем, о маршруте и ориентирах для движения, передаваемая всем остальным наблюдателям, следующим вне поля зрения объекта, с помощью радиопереговорного устройства или определенной системы условных знаков.

Второй наблюдатель, следующий непосредственно за ведущим наблюдение, действует как бы во втором эшелоне и не имеет, как правило, значительного контакта с наблюдаемым. В зависимости от местных условий, он держится на достаточной дистанции от первого наблюдателя, находящегося непосредственно возле объекта (на малолюдных улицах — подальше, в центре города — ближе), и приспосабливается к темпу его движения.

Система условных сигналов, по-видимому, относительно универсальна для всех, кто по тем или иным причинам занимается слежкой.

Она, естественно, исключает из арсенала слежки достаточно организованных преступных структур наблюдение через дыру, прожженную сигаретой в газете, или завязывание шнурков на обуви в момент, когда объект наблюдения останавливается или внезапно оборачивается к ведущему слежку.

Вопросы тактического согласования действий всех участников наблюдения могут решаться, в частности, при помощи следующих *условных знаков*:

1. Скрещенные за спиной руки у непосредственно ведущего наблюдение: "Наблюдаемый остановился и продолжает стоять на одном месте".

2. Правая рука согнута в локте и упирается в правое бедро: "Наблюдаемый повернул направо".

3. Левая рука согнута в локте и упирается в левое бедро: "Наблюдаемый повернул налево".

4. Пристальный взгляд на часы: "Наблюдающего необходимо сменить".

5. Одна рука на головном уборе или голове: "Наблюдаемый развернулся и идет в обратном направлении (т. е. существует опасность попасть в его поле зрения)".

6. Обе руки на голове или головном уборе: "Наблюдаемый потерян (ушел от слежки)".

Этот перечень можно продолжить. Но главное, что необходимо усвоить — распознав подобные хитрости по внешним признакам, можно вовремя заметить слежку.

Контакт между ведущими наблюдение и находящимися в автомашине может осуществляться по радиосвязи. Это более конспиративный способ, но и его нельзя назвать неуязвимым. В многолюдных местах ведущий слежку должен находиться достаточно близко от объекта наблюдения, и последнему может быть слышен звук работы передатчика. Сам факт переговоров с помощью радиосвязи очень трудно скрыть и от прохожих, и т. д.

Изменение места и обстановки слежки ведет к изменению тактики наблюдения. На малолюдных или безлюдных улицах и широких площадях наблюдатели следуют за объектом длиной колонной, на большом расстоянии друг от друга (так называемое наблюдение в одну линию), на многолюдных улицах это построение не исключает движения по противоположной стороне.

Довольно сложно обнаружить наблюдение, при котором организуется постоянное "обтекание" наблюдаемого: одни ведут наблюдение сзади, другие, постоянно забегая вперед, — спереди.

В случае ухода объекта из-под слежки ведущие наблюдение перестраиваются в так называемую цепь и буквально прочесывают всю местность. Район потери берется под наблюдение — в расчете на то, что объект наблюдения снова появится через некоторое время.

Крайне сложно вести слежку в многолюдных местах — в метро, на вокзалах, в аэропортах, на рынках, в больших магазинах

и т. д. Правда, поскольку подобные места позволяют приблизиться к наблюдаемому почти вплотную, степень полноты слежки значительно возрастает. Однако одновременно резко возрастает риск потери наблюдаемого из виду.

Поэтому преступники в подобных ситуациях поступают следующим образом. К объекту приближаются один-два наблюдателя, другие берут наблюдаемого в кольцо и контролируют все возможные выходы.

Радиосвязь в строениях из железобетона неэффективна, система условных сигналов из-за ограниченной видимости — тоже, поэтому наблюдающие в подобных местах чувствуют себя неуверенно. Кроме того, возрастает возможность обнаружения слежки, о чем также следует помнить потенциальным объектам наблюдения.

Особо следует остановиться на методах ведения слежки в ресторанах, кафе, барах. После неожиданного захода объекта в эти места наблюдающие вынуждены, спустя некоторое время, зайти за ним следом и попытаться расположиться недалеко от него. Не исключено, что для этого будет использована, как говорится, смешанная пара (мужчина и женщина).

Кстати, смешанное наблюдение может пригодиться в некоторых деликатных ситуациях, например, при посещении наблюдаемым мест общего пользования.

Приемом, который свидетельствует о высоком уровне подготовки представителей организованной преступности, занимающихся слежкой, является *контрнаблюдение*.

Цель контрнаблюдения — обнаружение факта наблюдения за преступниками со стороны представителей правоохранительных органов или других лиц.

Прежде всего, в процессе контрнаблюдения выявляется факт наблюдения, а значит, определенный интерес к отдельным членам или преступной группе в целом.

Далее выясняется, кто ведет наблюдение и с какой целью. Для этого сами ведущие слежку берутся над наблюдение и, образно говоря, из охотников превращаются в жертву. Понятно, что после окончания слежки за объектом лица, попавшие

теперь под контрнаблюдение, отправляются в места своего расположения. Их адреса, номера автомашин могут сказать о многом, в том числе и о возможности слежки.

Выявив наблюдение, сообщники объекта наблюдения могут прервать его насильственным образом, вплоть до причинения *телесных повреждений или лишения жизни* ведущих наблюдение. Но, как правило, после подачи условного знака о наличии слежки преступник, находящийся под наблюдением, пытается уйти от него.

При получении сигнала о том, что он находится под наблюдением, преступник может отказаться доводить до конца задуманные действия, изменить их или перенести на "более удобное время".

Обнаружение за собой слежки может быть использовано для доведения самой разнообразной дезинформации до наблюдающих.

Количество лиц, задействованных для контрнаблюдения, определяется задачами и методами, с помощью которых обнаруживается слежка, а также видом самого наблюдения.

Как правило, если ведется подвижное наблюдение, члены преступной группировки обговаривают с лицом, которое может попасть под это наблюдение, точный и согласованный по времени маршрут его передвижения.

Сообщники, которые будут осуществлять контрнаблюдение, располагаются в удобном месте по ходу его следования и внимательно наблюдают за всем происходящим. Зная признаки ведения слежки, они фиксируют и запоминают всех, кого можно заподозрить в причастности к этому процессу. Не остаются без внимания и автомашины, попадающие в их поле зрения (внешний вид, номерные знаки, отличительные признаки).

После прохода мимо них их сообщника они перемещаются в следующий пункт наблюдения и проделывают то же самое.

Так, сменив несколько мест, они получают определенную информацию, анализируют ее и в зависимости от вывода о том, есть слежка или нет, подают условный сигнал лицу, в отношении которого могла вестись слежка.

Для быстрого перемещения лиц, ведущих контрнаблюдение, используется автомобильный и иной транспорт.

О высокой степени организованности и подготовки членов преступной группы свидетельствует и уход их из-под наблюдения (после обнаружения слежки).

Приемы ухода весьма разнообразны. При подвижном наблюдении, например, при посадке в вагон поезда метро, троллейбус или автобус они стараются сесть последними. Традиционный прием ухода — использование всевозможных проходных дворов, парадных и черных ходов.

Вот типичный пример: преступник, находившийся в пассажирском поезде, обнаружил за собой слежку и понял, что может быть задержан. Он поступил следующим образом. По прибытии поезда на одну из станций он покинул купе и пошел из вагона в вагон, запирая при этом по ходу движения все двери тамбуров имевшимся у него ключом. Этот прием позволил ему уйти из-под наблюдения.

Эффективен и прием ухода из-под наблюдения с использованием средств маскировки. Например, наблюдаемый заходит в какое-то помещение и переодевается, наклеивает усы, бороду, надевает парик. Через некоторое время он выходит обратно (не исключается изменение походки) с совершенно измененной внешностью.

При подвижном наблюдении для ухода от наблюдения преступники часто используют автомашины.

Члены преступных группировок могут использовать и иные приемы и способы ухода из-под наблюдения. В ходе такого противоборства проверяются знания, подготовленность, умение применять приемы и методы наблюдения, выявляются личные качества противников, их техническая оснащенность, умение ориентироваться в сложных (так называемых нештатных) ситуациях.

Таков лишь общий перечень приемов достижения скрытности действий членов преступных групп, которые в конкретных ситуациях и местах могут видоизменяться, дополняться, совершенствоваться.

Методы деятельности преступных групп частично совпадают с методами представителей общеуголовной преступности, но при этом они имеют свои специфические черты и отличительные признаки, при наличии которых можно сделать вывод о том, что речь идет именно об организованной преступности.

Признаки деятельности организованной преступности. Условно их можно разделить на общие, характерные для региона, района, и частные, которые в сочетании будут свидетельствовать о том, что организованная преступность рядом и в ближайшее время возможны неприятности.

О появлении в данном регионе преступной группировки свидетельствуют следующие *общие признаки*:

— увеличение числа грабежей, разбоев, подготовка и совершение которых проводились квалифицированно, группой лиц;

— появление или учащение случаев вымогательства (рэкета), похищения заложников и т. п.;

— процветание игорного бизнеса, как правило, в одних и тех же местах, игра в "наперстки", "три листа" и т. п. на виду у правоохранительных органов;

— появление или учащение случаев мошенничества и насилия во время купли-продажи автомашин и других дорогостоящих предметов и товаров;

— появление среди жертв преступлений лиц, живущих на нетрудовые доходы;

— факты всевозможных так называемых уголовных "разборок", "сходок" и т. п.;

— факты экипировки преступников под представителей правоохранительных органов, "скорой помощи", аварийных служб и т. д., использование ими средств радиосвязи, боевого армейского оружия;

— наличие у преступников недоступной рядовым гражданам информации при совершении преступлений (промышленной, коммерческой или финансово-кредитной тайны).

Частные признаки условно можно разделить на признаки подготовки и признаки покушения (начала преступного посягательства) на здание и помещения фирмы.

Признаки подготовки к покушению:

— появление вблизи или на территории фирмы лиц с неестественным поведением, или проявляющих неоправданный интерес к деятельности фирмы;

— выявление попыток получить, например, в бюро технической инвентаризации техническую документацию о расположении здания и помещений, их планировке;

— факты подбора и использования окон квартир, домов, магазинов, кафе и т. п. для наблюдения за фирмой;

— опрос окружения о деятельности фирмы;

— обнаружение лиц, интересующихся сверх меры распорядком дня фирмы и режимом работы сотрудников;

— появление лиц, фиксирующих расположение здания и помещений фирмы, а также ее сотрудников (фото-, кино-, видеозаписи и т. д.);

— обнаружение лиц, проявляющих "нездоровый" интерес к сфере деятельности фирмы;

— проявление в окружении сотрудников фирмы лиц из преступной среды, пытающихся завести знакомство (расположить к себе) с ними или их родственниками;

— неоправданное поведение или повышенный интерес к делам фирмы со стороны во время или накануне перемещения или прибытия на фирму ценных грузов;

— попытки прорваться без надлежащего разрешения (при наличии пропускного режима) в здание и помещения фирмы или в нерабочее время;

— попытки проверить режим охраны, разбивая стекла, простукивая стены и т. п.;

— появление "по делам службы" на территории фирмы или неподалеку сотрудников полиции, МЧС и т. д., не внушающих доверия своим видом, поведением или без удостоверений личности;

— факты, свидетельствующие о возможном прослушивании телефонов фирмы и ее сотрудников или случаи "уточнения" номера телефона и его принадлежности;

— появление автомашин и их длительное пребывание в районе фирмы или их неоднократное появление без видимых причин для этого;

— попытки обнаружить и изучить систему сигнализации и конструкцию запирающих устройств.

Признаки возможного начала покушения:

— наблюдение за всеми сотрудниками фирмы вне службы одновременно;

— телефонные звонки (отвлекающие, угрожающие и т. п.) вне службы одновременно всем или части сотрудников фирмы;

— получение повесток, записок или иных документов и т. п. с просьбой (приглашением) явиться всем сотрудникам фирмы одновременно в определенное время в одно или различные места;

— поломки (повреждения при дорожно-транспортном происшествии) автомашин сотрудников фирмы;

— похищение (исчезновение) сотрудников фирмы или их родных и близких;

— иные непонятные, нетипичные ситуации в обычном ритме жизни фирмы и ее сотрудников.

Способы противодействия посягательствам на здание и помещения фирмы со стороны преступных группировок в основном определяются самими видами и методами посягательства и зависят от состояния режима охраны (если, конечно, он создан) и сил, его обеспечивающих.

Практически выбор способов защиты здания и помещений фирмы может выглядеть следующим образом.

С момента получения данных о том, что со стороны какой-либо преступной группировки проявляется повышенный интерес к делам фирмы и не исключена возможность посягательства, необходимо предпринять следующее:

1) провести анализ информации, как уже имеющейся, так и поступающей или специально добываемой;

2) по результатам оценки информации определить цели и поставить задачи, которые необходимо решить в процессе защиты;

3) выбрать силы и средства защиты, а также продумать порядок их привлечения и использования.

При этом обязательно моделируются возможные варианты посягательства и его отражения, выбираются оптимальный и запасной варианты действий.

В итоге анализа и оценки ситуации может быть принято несколько решений. Например, обратиться за помощью в правоохранительные органы, негосударственные организации или к частным лицам и предоставить им выбирать способ защиты.

Остановимся на ином варианте, предусматривающем использование собственных сил и создание режима охраны здания и помещений фирмы.

Поставив четкую цель, определившись с задачами, можно приступить к выбору способов, методов и принципов обеспечения режима охраны.

В данном случае имеются в виду общеизвестные методы и способы познания и противодействия неизвестному, которые с успехом можно применить в рамках режима охраны. Способы эти могут быть как активными (обнаружение и отражение посягательства), так и пассивными (предупредительные и аналитические).

Наиболее эффективно сочетание возможностей, предоставляемых государствам, частными структурами, и собственных сил и средств.

Разумеется, это будет стоить недешево, но всегда следует помнить — скупой платит дважды.

Многие фирмы стремятся при создании собственных служб безопасности (СБ) возложить на них, помимо функции обеспечения безопасности, разведывательные функции (причем для добывания информации не только защитного характера). И это естественно — сбор экономических и научно-технических сведений о конкурентах является одним из элементов существования в структуре рыночной экономики.

Поэтому несколько подробнее остановимся на идее использования собственной службы безопасности и рассмотрим основные, контурные элементы схемы ее возможного создания и функционирования.

1.3. Безопасность текущей предпринимательской деятельности

1.3.1. Анализ деловых предложений и контактов

Работа над любым проектом начинается с определения качества исходной информации. Поскольку она исходит от людей, начинать анализ следует с источника информации.

Работа с собственниками проекта

Непосредственными владельцами проектов могут быть либо их авторы, либо собственники, либо должностные лица корпоративных авторов и собственников. Более никто ни при каких условиях таковым считаться не может.

Работа с непосредственными собственниками проекта является наиболее эффективной, она приводит к более точным результатам. Поэтому лучшим вариантом будет тот, при котором клиент приглашает вашу фирму к участию в своем проекте с самого начала.

В этом случае можно применить методы безопасности для успешной диагностики состоятельности проекта уже на стадии предварительной проработки. Изначальная информация будет иметь высокие качественные характеристики. Взаимодействие может стать плотным и оперативным.

Работа с инициаторами проекта

Совсем другое дело — работа с чужими проектами. Здесь нужно тщательно работать с самого начала. Информация об инициаторах проекта часто может сразу же натолкнуть на нечто значимое.

Если это будут нехорошие подозрения, вас не должно удивить, что большая их часть подтвердится в дальнейшем.

Однако случаи работы с инициаторами предоставляются далеко не всегда. Очень часто приходится взаимодействовать только с представителями владельцев и авторов. На это может быть масса причин: нежелание фирмы засвечиваться, неудобство ведения дел иным способом и проч. Среди этих дел есть немало таких, о которых посредники либо молчат, либо попросту не знают.

Рассмотрим, что можно выяснить непосредственно от представителя. Подходы к верификации представителей носят универсальный характер и могут быть применимы не только для проработки проекта, но и в других работах, где приходится общаться через посредников.

Работа с представителем

1. ***Проверка уровня представительности.***

Прежде всего необходимо документальное подтверждение полномочий представителя. Фирма должна снабдить его доверенностью, в которой четко указывается, в каких пределах и что может совершать этот человек от лица фирмы, выдавшей доверенность. Реквизиты и атрибуты доверенности должны соответствовать общеупотребительным нормам.

Проверка в обязательном порядке должна включать диагностику фальсификации бумаги. Вместо доверенности может быть использовано служебное удостоверение, если человек утверждает, что он прибыл от фирмы и является ее штатным сотрудником.

Естественно, что речь идет о беседе вне офиса инициаторов и без предварительных проверок со стороны. Если фирма-доверитель — нормальная фирма, полномочия доверенного лица должны быть засвидетельствованы.

Если у инициатора нет доверенности, а он утверждает, что является агентом пославшей его фирмы, хорошие результаты дает ознакомление с агентским контрактом такого доверенного лица. Некоторые выказывают неудовольствие тем, что вы бу-

дете посвящены в условия их финансовых отношений с хозяином. Подобной "неловкости" можно легко избежать, если, например, попросить агента заклеить условия его оплаты бумагой или цветным скотчем.

Полезно уточнить характер взаимоотношений между представителем и его хозяином — это может пригодиться в дальнейшем. Представитель это прекрасно знает, поэтому лучше всего его добропорядочность характеризует факт передачи вам агентского контракта полностью. В любом случае следует настаивать на том, чтобы его показали. Ваши действия диктуются профессиональными требованиями, а не праздным любопытством, и доверенное лицо должно это понимать.

Если вы чувствуете, что человек упорствует, сами предоставьте ему какие-либо сведения. Необходимое документальное обеспечение у вас должно быть всегда под рукой. Вы как бы сразу же уравниваете взаимные позиции. *"Вы говорите, что представляете такую-то фирму? Отлично. Обменяемся подтверждениями"*.

Даже если вам с ходу кладут на стол визитку, это еще ничего не значит, вежливость вежливостью, но давайте работать. Понимающий человек не обидится, "непонимающий" может представлять угрозу.

В отдельных случаях можно обеспечить проверку иными способами, например, звонком в фирму представителя. Однако не следует забывать, что там может быть организован "автоответчик" (при серьезных аферах это делается почти всегда). Вежливый голос представится вам: *"Алло, фирма такая-то, здравствуйте..."* вы должны быть твердо уверены, кто перед вами и что за ним стоит. Иначе вы, как минимум, обречены на работу с "общественниками", доверенными доверенных или просто заблуждающимися.

2. ***Порядок информации.***

После знакомства с объектом необходимо проверить порядок информации, имеющейся в его распоряжении — сколько передаточных звеньев прошла информация и как она могла исказиться. Доверенное лицо фирмы, даже наделенное правом ведения пере-

говоров, в крупной игре фирмы-хозяина может быть использовано в качестве пешки. Ни правил игры, ни целей оно себе не представляет. Особенно это свойственно нашим доморощенным "фирмачам".

Даже ближайшие заместители могут не знать реальных замыслов директора, не говоря уже о доверенных лицах. Поэтому неплохо проверить надежность связей и проанализировать реакцию фирмы. Иногда по незначительным ответным реакциям можно составить совершенно точное представление о том, кто реально и с чем конкретно перед вами.

3. ***Деловой вес представителя в фирме.***

Это разновидность того, о чем говорилось выше. Переоценка делового веса представителя может иметь плохие последствия. Ведь некоторым своим сотрудникам фирмы доверяют лишь слабые проекты. И от такого представителя можно долго дожидаться результатов. И вполне вероятно, может оказаться, что эту работу параллельно уже кто-то выполнил.

Значимость делового веса представителя на порядок возрастает, если вы хотите от фирмы уникального решения, не свойственного ни ее профилю, ни текущему состоянию дел, ни прочим значимым внутрифирменным факторам. Все это в полной мере распространяется и на инициативы фирмы, проводимые через ее доверенное лицо. Так что необходимо прежде всего проверить статус данного человека в той фирме, которую он представляет.

Работа с посредниками

Наихудшие результаты показывает работа с цепью посредников. Насколько это плохо — знает каждый деловой человек, поэтому необходимо ознакомиться с приемом обнаружения цепочки посредников. Он называется "цейтнотной провокацией", и это отражает его основной принцип, в какой бы форме прием ни реализовывался. Поясним на простом примере, как строится и работает "цейтнотная провокация".

Посредник, предлагая найти недостающее звено для сделки, называет ценовые ориентиры и стимулирует интерес к тому, кого вам надо найти. При этом дается минимум стартовой информации и обещается предоставление подробностей после того, как отыщется недостающее звено. В такой ситуации многие воодушевленно отправляются на заработки — искать недостающее звено. Но, даже имея нужного человека, следует поступить иначе.

1. ***Загоните посредника в угол.***

Накануне выходных, например, в пятницу вечером, сообщите ему, что нашли нужного человека и он готов участвовать в деле. Вашему человеку требуется обещанная точная информация, но, естественно, через вас, вы тоже посредник "битый" и не выдадите свой "контакт".

Настаивайте на том, что все переговоры вы будете вести только лично с посредником, и ни с кем более. Обострите ситуацию тем, что информация нужна как можно быстрее, а не то ваш человек вот-вот уедет. Единственное, в чем вам надо быть уверенным, — что у вашего собеседника этой информации нет. Любой посредник без проблем вычисляется по деталям при первой же беседе, даже если ему очень хочется выглядеть главной фигурой.

2. ***Анализируйте реакцию посредника.***

Если посредник соглашается на встречу сразу же, например, вечером в пятницу или субботним утром, — очень хорошо. Возможно, он действительно единственный посредник. Высока вероятность качественной информации, если это не сознательная дезинформация.

Если посредник назначает встречу на начало следующей недели, с утра, это также неплохо. По всей видимости, он имеет возможность созвониться с инициаторами в выходные, т. е. те доверили ему свои номера домашних телефонов. Возможен неплохой представительный уровень, цепь маловероятна.

Чем дальше отодвигается срок встречи — тем хуже, тем больше народу в цепочке посредников, тем слабее связь с истинными инициаторами, тем меньше должна стать мера вашего доверия

посреднику. Если при этом вы получаете хоть какие-то ссылки на объективные трудности (затрудненность связи, отсутствие инициаторов, командировка и т. п.) — смело ставьте крест на такой затее.

Редкий посредник сознается, что в деле, оказывается, много народу и его номер — всего лишь шестнадцатый. Ваш блеф трудно вычисляем, так как "найденное" вами лицо в любой момент может "отказаться от участия в проекте", а вы как профессиональный посредник не обязаны "сдавать концы". Только после прощупывания посредника можно серьезно выслушать его предложения.

Анализ контакта

Итак, кто-то пришел к вам или вашему клиенту с делом. В таком случае можно говорить о "контакте" — новых открывающихся перспективах, возможностях и... разведывательной деятельности.

Чем скорее вы сориентируетесь, что перед вами, — тем лучше. Выше рассмотрено, что может дать поверхностный анализ статуса пришедшего. Сейчас давайте уточним, как можно проанализировать факт контакта без проработки сути стартовой информации.

Предпринимательская практика показала, что анализ контакта полезен для определения серьезности намерений инициаторов. Мотивация контакта должна быть строго определена не столько для построения дальнейшей деятельности, сколько для ее вероятного прекращения.

Анализ контакта должен дать ответ на простой вопрос: "Насколько случайно на вас вышли?" Случайность, как правило, работает в худшую сторону. Поэтому любые случайные инициативные контакты подлежат расследованию. Особенно это касается фирм, не стремящихся афишировать свою деятельность.

1. ***Поручительство.***

С первого контакта следует уточнить, как вышел на вас инициатор. Побеседуйте, порасспросите. Вам должны быть даны

исчерпывающие и четкие объяснения по поводу того, как и кто вывел инициатора на вас. Анализ поручителя может дать полезную информацию. Если, например, ссылаются на вашего бывшего партнера, который и порекомендовал обратиться к вам, — это очень хорошо. Правда, у вашего партнера мог быть совершенно случайный контакт с этим инициатором, но в беседе с вами он трактует этот контакт уже по-другому. Уточните этот пункт. Наведите справки у того, на кого ссылается инициатор.

2. ***Надежность намерений инициатора.***

Проверкой контакта предугадывается серьезность намерений инициатора. Однако имейте в виду, что, даже если вы делаете вывод о кажущейся серьезности контакта, это всего лишь предварительный вывод. Считайте просто, что инициатор успешно прошел первый рубеж вашей обороны. Говорить о гарантиях надежности намерений еще очень и очень рано.

3. ***Степень доверия инициатору.***

Необходимо сделать вывод, что если и не все сказанное данным лицом будет в дальнейшем соответствовать истине, то, во всяком случае, этому есть объективные предпосылки. В этом случае самое пристальное внимание должно быть уделено возможности подсадки в вашу фирму чужого агента, и нужно приготовиться к противодействию. Здесь мы входим в область прерогатив службы безопасности.

Легендирование проекта

Назначение и методология легендирования

Легендирование — это дезинформирование противника с целью сокрытия своих истинных мотивов, направлений деятельности. Когда оперативный работник произносит слово "легенда", всегда имеется в виду своя или чужая ложная информация, призванная скрыть истинное положение вещей.

Легендирование известно давно и применяется сегодня столь же активно, как и прежде. Легендирование стало явлением повсеместным и широкомасштабным.

Субъектов легендирования можно встретить везде и всюду: от посетителей фирмы до глав государства. Везде, где есть необходимость технически грамотно скрыть истину, можно обнаружить применение легендирования.

Даже в нормативном бизнесе, сознательно избегающем элементов лжи и дезинформации, непредумышленное легендирование в силу личных амбиций невольных создателей легенд привносит в деловую жизнь искажения реальности, что рано или поздно приводит к вполне ощутимым проблемам.

По преследуемым целям деловое легендирование можно условно разделить на несколько групп:

1. *Манипулирующее, или стимулирующее, легендирование* призвано создать в сознании объекта устойчивое ощущение реальности происходящего и стимулировать либо пресекать активные действия. В этом варианте легенда может не очень сильно отклоняться от истинного положения вещей, но отдельные фрагменты могут быть сильно деформированы. Такая тактическая уловка гасит возможные сомнения объекта и подталкивает его к действиям либо воздержанию от таковых.

Нелишне заметить, что стимулирующее легендирование может служить средством манипулирования не только отдельным объектом, но и солидными их группами. Это можно наблюдать в деятельности различных трастовых компаний, привлекающих огромные ресурсы личных сбережений в обмен на низкоинформативные обещания.

Эти вот туманные обещания и являются легендой деятельности. При этом легенду могут усилить непосредственно оперативными путями, например, пустив слух через брокеров и трущихся в толпе агентов о неких грядущих таинственных "операциях".

2. *Отвлекающее легендирование* применяется для создания у объекта ложного представления о сути дела и отвлечения внимания, направления его в другую сторону от засекречиваемой или нежелательной информации.

Технология создания и внедрения легенды

В основе легендирования деятельности лежат несколько проверенных временем психологических механизмов. Рассмот-

рим пример возможной обработки вами некоего провинциального банкира. Задача — убедить его, что вы представляете серьезную фирму, и дать вам кредит. Какова будет механика создания и воздействия легенды на объект?

Во-первых, активно используется *свойство избирательности человеческого восприятия*. Мы видим только то, что можем распознать и что присутствует в нашем прошлом опыте. Поэтому, например, ссылка в разговоре на "бенефициарные отношения между нашей фирмой и лондонским банком-корреспондентом" для большинства собеседников малопонятна.

Однако для того, чтобы они посчитали фирму авторитетной, этого может оказаться вполне достаточно. Реагируя на знакомые значимые слова автоматически, т. е. с опорой на прошлый опыт и знания, объект может пропустить главное — легенду. Восприятие информации по внешним признакам без ее осмысления — один из объективных законов, весьма широко эксплуатируемый манипуляторами всех времен и народов.

Если вам удалось хоть раз внедрить такую полуинформацию в сознание оппонента, будьте уверены, что его возможные сомнения рассеются. Он поместит вашу фирму на одному ему ведомую полочку собственного сознания с надписью: "Крутые ребята" — и даже, скорее всего, скоро забудет, почему он это сделал.

Далее вам надо только поддерживать такой имидж. Он уже зажил собственной жизнью и работает на вас. И на то есть вторая по степени значимости причина. Работает *психологическая защита человека*. Самая грубая ложь легко нивелируется, утрачивая свою значимость, если сам объект не хочет ее видеть. Пожалуй, даже правильнее сказать так: хочет не видеть.

Продолжим пример обработки объекта. Даже если в предлагаемом вами контракте нет ни слова про какой-то там лондонский банк, однажды уже примерившись к вам и создав о вас представление, ваш объект навряд ли решится пересмотреть собственные оценки. Он уважает себя и свой профессионализм. Он по-прежнему будет уверен, что вы — фирма серьезная, работающая в интернациональном масштабе.

Попробуйте на своих знакомых, и вы убедитесь, что самооценка стоит выше осторожности и защищается намного сильнее. Даже если вы допускаете ошибки, нормальный человек скорее будет придумывать им оправдания, нежели допустит пересмотр собственных оценок, тем самым поставив под сомнение репутацию своего "Я". Игра амбиций чревата заблуждениями, которые, как туман, в один прекрасный момент могут подвести к краю пропасти.

Третий фундаментальный камень построения легенды — *вера человека в значимость других*. У каждого из нас есть круг лиц, мнению которых мы верим. Механика такого доверия базируется в основном на первых двух рассматриваемых нами принципах. Но, в отличие от них, здесь присутствует еще и социальный эффект. Мы больше доверяем тому, что касается нашей социальной группы, нежели нас непосредственно. В толпе, коллективе, группе мы делаем такое, о чем наедине и подумать страшно.

Продолжим пример с обработкой банкира: в подкрепление легенды о серьезности своих намерений вы можете продемонстрировать благодарственное письмо из Н-ской губернии, в котором вам сообщается, что благодаря вашим же стараниям удалось успешно провести посевную, — и ваш объект будет счастлив от сознания своего участия в большом деле.

Проверка результатов легендирования

После того, как вы внедрили свою легенду в сознание объекта, необходимо быть уверенным, что это надежно. Поэтому нужно знать определенные признаки, характеризующие нужную глубину доверия вашего объекта вам и вашей информации. Глубина определяется характером реакции. В нашем случае такими признаками являются встречные предложения банкира.

Вы получаете оценку "пять", если банкир просит о личных услугах. Здесь особо ценится намерение банкира лично поучаствовать в деле. Оценка "четыре" соответствует готовности банкира предоставить кредит без дополнительных запросов и проверок фирмы. Оценка "три" соответствует принятым стандартным запросам банка.

Изобличение чужой легенды

Не будем заострять внимание на очевидных проколах при проверке легендирования поиском внутренних и внешних противоречий. Это в состоянии сделать и делает любой нормальный человек. К этому готовятся и манипуляторы. Вместо этого ознакомимся с психотехникой обнаружения и дешифровки чужих легенд.

Для начала предположим, что в любой легенде должны присутствовать неизбежные черты человеческого несовершенства. Попробуем их рассмотреть. Как эксплуатировать психологические проколы для изобличения легендирования в чужой игре? Например, в ситуации, когда вы работаете против инициаторов сомнительных проектов.

Хорошая легенда должна исчерпывающе объяснять поведение и мотивы объекта, давая правдоподобные объяснения на ваши возможные вопросы. Исходя из этого, создатели легенд стремятся предусмотреть круг и характер возможных вопросов. При этом манипуляторы стремятся охватить вниманием, как правило, достаточно ограниченное поле ваших сомнений. По большей части такое поле представляет собой стереотипные наборы традиционных в данной ситуации вопросов.

Здесь и заложена возможность обнаружения легенды. Достаточно сформулировать вопросы, выходящие за рамки стандартных, чтобы чужая легенда зашаталась.

Если на ваши неожиданные вопросы вы сразу получаете ответы, объясняемые или подтверждаемые предлагаемой вам легендой, возможен один из двух исходов: первый — доверие легенде повышается и есть вероятность истины, второй — вы имеете дело с тщательно разработанной легендой, которую не так-то легко нащупать. В любом случае подобная процедура полезна и не надо ею пренебрегать. Тем более что такая работа не требует каких-либо значительных усилий.

В обиходной практике признаками легендирования могут быть следующие:

• отлынивание под всяческими благовидными предлогами от предоставления дополнительной уточняющей информации;

• игнорирование и замалчивание части ваших вопросов.

Легенде часто сопутствуют общие признаки манипулятивного и лживого поведения. Также часто можно видеть признаки агрессивного поведения.

Реакция на факт установленного легендирования

Итак, вам удалось обнаружить, что человек, сидящий перед вами, мягко говоря, не то, что есть на самом деле. И он прилагает усилия к тому, чтобы вы этого не заметили. Что делать дальше с этим персонажем? Все зависит от ситуации и поставленных задач.

Путь первый — занести объект и значимую информацию в "черный список" на будущее и прекратить отношения.

Путь второй — затеять с объектом игру, сделав вид, что все, что он вам наговорил, вами проглочено; такая стратегия при внешней рискованности иногда может привести к весьма эффективным результатам.

1.3.2. Ведение переговоров

Начало переговоров

Распространенное начало предпринимательского проекта — устные переговоры. Теоретически намерения пришедших сводятся к поиску возможного партнерства и устному закреплению опорных моментов, которые в дальнейшем должны переродиться в учредительские документы либо контракты. На практике же намерения могут быть совсем иными.

Для СБ (подразделений разведки и контрразведки) устные переговоры — богатый материал и широкое поле деятельности. В подавляющем большинстве случаев диагностика фальсификаций может быть выполнена и выполняется именно на этапе первых переговоров. Основная масса гипотез и рабочих версий СБ рождается на переговорах. СБ должна применить все свое умение, все рабочие навыки и приемы для квалифицированного контроля и анализа получаемой в ходе переговоров информации.

Совершенное искусство переговоров подразумевает свободное владение дисциплинами оперативной психологии, такими, как приемы коммуникации, физиономистика, анализ речевых характеристик, знание и видение вазомоторных реакций человека, использование всего многообразия приемов и средств, наработанных в сфере манипулирования и модификации поведения.

И это оправданно. Напомним, что главное предназначение СБ — уберечь фирму на ранних подступах к "минному полю". Цель — распознание слабых сигналов беды. Нужно и должно работать и тогда, когда внешне все мирно и спокойно.

План переговоров

До начала переговоров необходимо разработать план, включающий несколько сценариев возможного развития беседы. При этом его условно можно разделить на две группы:

1) "бизнес" — то, что будет говориться в интересах бизнеса;

2) "СБ-мероприятия" — что будет делать служба безопасности.

Первую часть плана необходимо детально обсудить с руководством фирмы. Нехорошо, если в беседе возникнет необходимость отговорки типа "*я должен проконсультироваться или согласовать*" или просто "*не знаю*". Это явно черный крестик и потеря авторитета для СБ со всеми вытекающими последствиями. На крайний случай можно прикрыться фразой типа "*это вне моих полномочий на сегодня*". Такая позиция может явиться преддверием оперативных игр с объектом.

При подготовке плана переговоров следует определить их главную цель.

Согласно последним разработкам науки о конфликтах, переговоры могут быть следующих типов:

- "разведка" — прощупывание позиций сторон; цель переговоров — получение исходной информации к дальнейшему взаимодействию;
- "война" — стороны разделены непримиримыми стратегическими противоречиями; цель — победа одной стороны за счет другой;

• "дебаты" — стороны противостоят на тактических позициях; возможен компромисс;

• "игра" — стороны преследуют сугубо оперативные цели в виде соблюдения установленных и незыблемых правил; цель переговоров — сами переговоры.

Понимание типологии предстоящих переговоров помогает построить план дальнейших действий. Рассмотрим первый, наиболее актуальный вариант: обращение к фирме как к возможному партнеру.

Рекомендации также применимы и для обратной ситуации, когда фирма обращается к другой в качестве инициатора деятельности. Смысл не меняется, если помнить о том, что любая рекомендация имеет двойную ценность — средства введения в заблуждение других, если ее применяете вы, и средства своевременного обнаружения таких действий, если их применяют против вас.

План переговоров для данного варианта один — слушать и смотреть. Но — глазами СБ.

Подготовка к переговорам

1. ***Состав группы.***

Ввиду высокой информационной насыщенности первичных переговоров рекомендуется проводить их силами рабочей группы.

Если в структуре СБ присутствуют узкие специалисты, нужно позаботиться об их совместной деятельности хотя бы на первой встрече. Задача — не упустить ни крупицы информации. Все, что может быть получено на первых переговорах, — бесценный материал. Второй такой возможности может и не представиться.

Основная рабочая единица на переговорах — двойка или тройка сотрудников. Обязанности делятся в соответствии с личной умелостью работников и целями предстоящей беседы. Обычно на переговорах лидирует один — "торпеда", второй сотрудник отслеживает реакции оппонентов, третий следит за ходом развития беседы, осуществляя общее руководство тройкой в ходе бесед.

Такое разделение функций позволяет эффективно собирать и обрабатывать информацию без риска высветить оперативную направленность деятельности.

Также имеется много других ролей, возлагаемых на членов группы переговорщиков с точки зрения СБ. Например, классическая двойка "плохой — хороший" представляет собой сочетание ролей сговорчивого, компромиссно настроенного, миролюбиво-уступчивого переговорщика и его непримиримо-твердолобого, агрессивного партнера.

Работа такой двойкой позволяет всесторонне прощупывать позицию инициатора без привлечения дополнительных ресурсов. Такая пара имеет обширный оперативный простор как по формам воздействия, так и по силе.

Замечание. Каждый человек имеет свою манеру ведения переговоров, отражающую черты его характера. Условно говоря, один умеет ругаться, второй — нет, один склонен красиво уступать, второй делает это так, что тактическое отступление становится равным полному поражению. В зависимости от целей переговоров и принятой тактики может оказаться полезным привлечение к переговорам нужного "характера".

2. ***Внешний облик.***

Составив себе представление о мотивах инициаторов, например по информации о сути предстоящей встречи, можно смоделировать требуемое восприятие, обратившись к соответствующему имиджу.

3. ***Экипировка.***

Все переговоры в обязательном порядке должны быть записаны. Поэтому при подготовке к разговору на чужой территории следует заготовить необходимую технику.

4. ***Время подъезда.***

Управление временем — черта однозначная. Опоздал — значит, специально хотел опоздать или не очень хотел успеть. Опоздание на встречу сверх разумного для демонстрации важности и значимости дел — дешевое манипулирование. Подразумевается незначительность лиц, к которым вы соизволили прибыть с опозданием.

5. ***Размещение.***

При размещении переговорщиков необходимо обеспечение расширенного поля внимания. Расширенное поле внимания подразумевает активную концентрацию внимания на деталях, расширение угла обзора для использования бокового зрения и специфичные методы фиксирования взгляда. Когда это применяется СБ?

Во-первых, при визуальном наблюдении за объектом. Эффективность наблюдения напрямую связана с тем, насколько четко и грамотно фиксируются внешние проявления объекта — будь то двигательные реакции, изменение мимики, жестикуляции или прочих контролируемых параметров объекта.

Во-вторых, иногда интересующая информация находится вне поля вашего зрения. Например, при проведении переговоров необходимо контролировать выражение лица не только говорящего, но и его компаньонов, сидящих по разные стороны.

В-третьих, фиксация взгляда необходима для эффективной техники общения. Грамотно поставленный взгляд дает большое подспорье тому, кто им владеет. В комплексе с известными способами обработки объекта управлением взглядом можно достигать различных эффектов: от создания у объекта чувства дискомфорта до стимулирования требуемых позитивных эмоций.

Размещение переговорщиков зримо показывает отношение инициаторов к вашей группе как таковой и к конкретным персонажам в частности. Если вам предлагают перейти на диванчики вокруг столика, это предусматривает доброжелательное отношение ко всем вам? Или просто хотят отвлечь ваше внимание?

Если оставляют всю команду за огромным столом, скорее всего, дают понять, кто тут главный. Иногда референт или другое лицо, обслуживающее переговоры с той стороны, может персонально усаживать каждого.

Подумайте, какую позицию предлагают занять конкретно вам и почему? Все ли переговорщики с той стороны находятся в пределах вашей досягаемости? Как вы выглядите в плане доступности для их наблюдений? Если вы оказались в невыгод-

ном положении один из всей команды, возможно, у той стороны есть поводы для подозрений персонально к вам? Вас дешифровали и показывают это?

6. ***Свет.***

В этом аспекте переговоров небезынтересно рассмотреть использование освещения. Бывает так, что вас стремятся усадить таким образом, чтобы свет падал вам в лицо. Кое-кто поизощреннее может уже после рассадки включить специальное освещение, про которое вы и не подозревали ранее.

Пересаживаться может быть неудобным, но ваш визуальный контроль отключают тем же выключателем, каким включают лампы. Попытки создания у вас дискомфорта ненавязчивым направлением света вам в лицо — не более чем дешевая уловка. Можно посоветовать "пройтись" по этому поводу и нагло пересесть в кресло референта.

Что делает СБ, сопровождая своего шефа на переговорах?

1. ***Фиксирует происходящее.***

Запись и наблюдение за беседой должны стать непреложным правилом. Не нужно пытаться принимать активное участие в беседе и что-то анализировать, в эти моменты аналитические возможности понижены. Необходимо всеми способами стремиться к тому, чтобы увидеть и услышать как можно больше. Желательно применять записывающую технику.

Необходимость записи беседы связана с так называемой доказательной базой. В обязательном порядке нужно постоянно создавать и поддерживать доказательную базу достигнутых соглашений. Предположим худшее: дело дошло до скандала.

Как показывает практика, иногда одна обрывочная запись может стоить показаний десятка сотрудников фирмы. Противной стороне может оказаться достаточным обвинить их в сговоре или в корыстном интересе.

2. ***Осуществляет скрытное наблюдение.***

Наблюдение за жестикуляцией переговорщиков представляется весьма эффективным средством дешифровки чужого по-

ведения. Особенно когда они обмениваются специальными сигналами, что весьма часто сопутствует ненормативному бизнесу. Часто группа переговорщиков использует жестикуляцию для обмена мнениями по ходу беседы и соответствующих корректировок планов.

Если удастся понять, что стоит за почесыванием подбородка и как протирание очков босса противника изменяет направленность беседы, — это очень хорошо. Диагностировать подобную сигнальную систему нетрудно. Достаточно обратить внимание, на что постоянно смотрят члены команды, какие движения могут повторяться без видимой нужды. Возможно, именно такие знаки просигналят о самом важном в позиции противника.

Завершение переговоров

Чем больше СБ общается с противником, тем больше шансов на успех. В зависимости от опыта, личностных характеристик, текущих позиций сторон уполномоченные лица, ведущие переговоры, могут водить за нос друг друга до бесконечности, что для многих иностранных бизнесменов, впервые столкнувшихся с реалиями славянского бизнеса, совершенно непонятно. СБ же делает это исключительно с целью уточнения и проверки своих собственных гипотез.

В странах устоявшегося бизнеса единожды произнесенное обещание в присутствии свидетелей либо с иной доказательной базой (запись телефонного разговора или даже пометки в блокноте) может оказаться достаточным для возбуждения дела о взыскании убытков. Обещал — делай. У нас все иначе. От обещаний до дела порой может пройти вечность, а потом вдруг вас поставят перед фактом выполнения совсем не того и не так, как вы договаривались.

Лучше вообще воздержаться от обещаний чего-либо от имени других лиц, сколь бы вы ни были в них уверены. Иначе вас рано или поздно автоматически отнесут к несерьезным партнерам.

В последнее время особенно заметна тенденция: в мире крупного предпринимательства мера ответственности за данное слово уже-

сточается день ото дня. Кроме того, в различных криминальных схемах денежных болтунов ловят за длинный язык.

Специфические рыночные регуляторы в виде "крутых братков" на самом деле — нездоровая реакция на нездоровую деловую практику. Дыма без огня не бывает. Кровавые разборки, столь частые сегодня, не бывают спонтанными и немотивированными.

Во избежание неприятностей — кто бы вы ни были — ни одного необдуманного обещания малознакомым партнерам!

Никаких выводов, никаких обещаний, никаких решений. *"Мы подумаем"* — вот самое большее, что следует сообщить своим визитерам, сколь бы заманчивым вам ни показалось их предложение. *"Мы обсудим ваше предложение и в самое ближайшее время встретимся еще раз"* — только это можно сказать на прощание, покидая чужой офис. Обратите внимание: фраза типа *"мы дадим ответ"* отсутствует. Пусть слушают свои записи... А подобная фраза в конце беседы — промах.

Есть простой способ убедиться, что ваше предложение представляет интерес: в конце переговоров постарайтесь замять вопрос, кто первым выйдет на связь, ограничьтесь фразой типа *"давайте созвонимся такого-то числа"*. Если ваше предложение заинтересовало — вам позвонят сами.

После завершения переговоров следует обратить внимание на то, как вас провожают. До выхода из кабинета, до поста охраны, до вашей машины? Кто именно это делает? Все это внешние сигналы результативности переговоров.

Что именно говорят на прощание, какими словами и как? Что делают, когда вы расселись по автомобилям и тронулись в обратный путь: снимают улыбчивую маску и уходят или стоят, глядя вам вслед, пока вы не скроетесь из виду? Вообще, наблюдения за "последействием" — одни из наиболее показательных. Манипулятор, отворачивая от вас лицо, обязательно его изменит.

Что нужно выполнить после проведения переговоров?

1. Провести анализ полученной информации. Выделяются возможное легендирование, спорные и противоречивые моменты стар-

товой информации. Весьма эффективно для проведения разбора переговоров использование магнитофонной записи беседы.

2. Все визуальные наблюдения за противником, включая анализ поведенческих реакций, нужно проанализировать, обобщить для построения психологических портретов объектов.

В случае обнаружения подозрений СБ информирует руководство фирмы с соответствующей мотивировкой. Например: вас мистифицируют или пытаются злоупотребить вашим вниманием. Здесь может пригодиться запись беседы. В отдельных вариантах может понадобиться проверка инициаторов.

3. Общее впечатление о чистоте намерений инициаторов и стартовой информации будет представлять итог первичных наблюдений.

4. Следует построить прогнозы возможного негативного развития ситуации, совместив спорные моменты и подозрительные наблюдения с имеющейся информацией. Версий может быть выдвинуто множество, важно выбрать подходящие методы проверки информации и потенциальных противников.

Когда можно обойтись без проверки стартовой информации? Почти никогда. Даже если видны явные попытки манипулирования, имеющие однозначно неподходящие или угрожающие мотивы, либо предлагаемое дело совершенно неинтересно, все же стоит задуматься о реальных целях инициаторов, о том, не было ли у них скрытых мотивов.

Возможно, кто-то прощупывает дело? Возможно, где-то протекла нежелательная информация? Всегда есть пища для раздумий.

1.3.3. Проверка состоятельности проекта

Следующим (после установления добросовестности инициаторов) этапом работы над любым деловым предложением (проектом) является оценка его выгодности. И на этом этапе, который по терминологии ведущих специалистов по экономической разведке в современном российском предпринимательстве называется ***механизмом образования дохода (МОД)***, роль СБ весьма важна.

Работа начинается с проверки планируемого дохода. Верификация дохода является краеугольным камнем проведения экспертизы любого проекта, нацеленного на прибыль.

Каковы основные признаки доходности проекта?

1. ***Формула успеха.***

МОД описывает объективную возможность получения дохода. Объективность требует проверки. Конкретизируя экономическую состоятельность МОД, его цифрами наполняют такие показатели, как прогноз прибыли, затрат, рентабельности и т. д., отражаемые в технико-экономическом расчете или обосновании проекта (ТЭР или ТЭО).

С практической точки зрения МОД и ТЭР удобнее рассматривать отдельно друг от друга. Иногда достаточно прийти к выводу о принципиальной порочности генеральной идеи, чтобы сэкономить массу времени и сил на ненужных расчетах и мероприятиях по их проверке. Количественная проверка должна следовать строго после качественной. Идея данного проекта принципиально жизнеспособна? Только после положительного ответа на этот вопрос можно переходить к вопросу: насколько?

Скрупулезный качественный анализ МОД, выявление и обследование его слабых и сильных сторон может привести к пониманию необходимости иного подхода к делу, что часто не только перечеркивает все предоставляемые расчеты, но и в корне меняет судьбу проекта. Очень часто работа на этом этапе оказывается весьма плодотворной.

Генеральная идея дохода должна формулироваться предельно четко и лаконично, отражая формулу рождения добавленной стоимости.

2. ***Секретность.***

Генеральная идея дохода по известным причинам часто засекречивается. Это могут быть различные соображения безопасности коммерческого, технологического или интеллектуального плана. Отметим, что МОД весьма часто является предметом опеки и охра-

ны со стороны собственника проекта. Это в первую очередь касается проектов повышенного риска и криминально-пограничных.

3. ***Инвариантность.***

Третья черта МОД проистекает из конструкции предпринимательского проекта. Основным признаком, характеризующим генеральную идею, является ее доминирование над всеми прочими идеями, присутствующими в проекте, что проявляется в инвариантности генерального решения по отношению к прочим частным решениям.

Например, если исследуется возможность реализации на рынке России нового стирального порошка зарубежной фирмы, то в областях локальных решений, таких, как ценообразование, постановка рекламно-информационной кампании, стратегия продвижения товара и т. д., возможны варианты, но только это будет связано с данным стиральным порошком данной фирмы.

Почему следует выделять МОД из общего бизнес-плана или функционирующего дела? Попробуйте проанализировать известные вам лопнувшие проекты, и вы убедитесь, что очень часто причиной их несостоятельности явилось невнимательное отношение к проработке стартовой идеи. У тех, кто игнорирует правило "зри в корень", рано или поздно начинаются проблемы.

Экспертиза МОД

Экспертиза МОД нужна в первую очередь там, где возникают любые посягательства на собственность, где инвестора бомбардируют всевозможными предложениями и необходима выработка оперативных решений. С точки зрения предпринимателя, экспертиза МОД — это обследование сердца затеи на предмет его вероятной остановки или наличия врожденных пороков. Такие убийственные вещи, как показывает практика, по большей части закладываются на этапе задумки идеи.

Рассмотрим ключевые характеристики МОД, отличающие плохой бизнес от очень плохого:

1. ***Автономность.***

Автономность — степень социализации проекта: насколько механика прибыли зависит от выполнения операций сторонни-

ми силами. В идеале в наших сегодняшних условиях лучшим проектом будет такой, при котором всю необходимую прибыль можно создать собственными силами. Натурализация хозяйства вчера, сегодня и, наверное, завтра еще останется одним из ключевых показателей надежности дела. С этих позиций хорошей будет та идея, при которой основная масса прибыли рождается в недрах предприятия — инвестора проекта. Исходя из этих соображений стартовая идея может быть поправлена.

2. ***Пластичность.***

Пластичность — возможности, заложенные в самой идее "делания денег". Насколько механика дохода нацелена на один-единственный вид деятельности, один-единственный продукт. Например, мини-завод по производству детских колясок по своей пластичности уступает набору модулей для того же производства. Что, если придется резко перенастраивать производство? Насколько идея учитывает этот фактор?

3. ***Системность идеи.***

При рассмотрении идеи нового дела необходимо оценить его с позиции системности, включая возможность наращивания оборотов и развития дела, воспроизведения и тиражирования полезного эффекта.

Уникальная разовая технология для принятия ее к воплощению должна обладать редкой финансовой мощью. Однако такой ограниченный подход отметает сильные системные ходы. Именно среди них, как показывает зарубежный, да и наш отечественный опыт, как раз и находится все самое стоящее, что достойно усилий и вкладов и что не зазорно оставить потомкам.

Кроме количественных показателей, индустриализация идеи МОД несет и качественные характеристики, в числе которых лидирует такая, как пригодность дела к работе без непосредственного участия инициаторов.

Нежизнеспособна идея, ориентированная на реализацию только при условии участия неких конкретных лиц. (Так же обстоит дело и в области полулегального бизнеса.) "Белоснежный бизнес", ориентированный на "человека-торпеду", также имеет низкие показатели

устойчивости и надежности. С ростом зависимости дела от конкретных фигур оно рано или поздно обрушивается.

Есть очень простой прием проверки объективности идеи: просто поменяйте фамилии исполнителей местами в функционально-операционном списке и посмотрите, что получится в итоге. Если результат неизменен, планируемое дело объективно. Чем более ощутимы проблемы, вызванные заменой хоть одного исполнителя, — тем менее объективно дело.

4. ***Временные показатели.***

При оценке временных параметров обычно выделяют следующие ключевые позиции:

• жизненный срок МОД. Как нетрудно видеть, есть дела-однодневки, есть дела на несколько лет, а есть — вечные. С ростом уровня инвесторов, с формированием инвестиционных принципов и политики жизненный срок МОД выдвигается в ряд первостатейных проектных признаков. Далеко не всегда "однодневка", даже сулящая баснословные прибыли, получает приоритет в инвестиционном портфеле. Серьезные предприниматели также приходят к пониманию этого подхода;

• время реализации МОД. Отражает продолжительность воплощения идеи, включая время на раскрутку проекта и настройку дела до вывода в оптимальный режим. Это — вторая по значимости временная характеристика. Сама по себе она мало о чем говорит. Ценность ее в том, что она позволяет инвестору сориентироваться в отношении возможных сроков движения денежных потоков.

5. ***Место зарождения дохода.***

Анализ места зарождения дохода может отражать врожденную слабость проекта. Часто интуитивно нащупанное направление имеет не самые сильные конечные решения. Ориентиром вполне может служить место зарождения дохода.

6. ***Экономическая мощность.***

Следует еще раз подчеркнуть, что сейчас рассматривается МОД проекта исключительно в целях качественного поиска слабых мест, снижающих или лимитирующих его экономическую мощь.

Мощность МОД может быть оценена приблизительно по принципу эффективности вложений: сколько можно получить на единицу вложенных средств? Исходя из этого, можно приблизительно оценить такие критерии, как "запас хода" — пластичность вероятного дохода, возможность снижения себестоимости, наличие люфтов-подвижек для принятия в долю необходимых участников. Если всего этого нет, проект автоматически попадает в разряд неблагополучных.

Отчасти при оценке экономической мощи МОД нелишне рассмотреть его с точки зрения маркетинга. Иногда именно МОД определяет такие качества, как, например, потребность и расходимость товара, жизненный срок, узнаваемость и готовность к покупке вероятными потребителями. Продукция массового спроса без труда "побьет" единичные уникальные изделия.

Примерно так же среди массовой продукции предмет длительного потребления уступает изделиям с коротким жизненным сроком. Среди краткосрочных продуктов проект, связанный с импортом продуктов питания первой необходимости, будет иметь больше шансов быть инвестированным, нежели, скажем, импорт роскошных вин.

Среди продуктов питания какие-нибудь крупы и макароны могут представлять гораздо больший интерес для инвестора, чем растворимые витаминизированные каши мгновенного приготовления. На чем стоит заострить внимание?

На распространенной оплошности, допускаемой почти всегда: на этапе экспертизы МОД часто приходится слышать некие обобщающие маркетинговые выводы типа "пролетарский продукт всегда уходит со свистом" или "пили, пьют и будут пить". Такая бизнес-демагогия чревата неприятностями.

Сам маркетинг еще только предстоит, а выводы уже сделаны, высказаны и оказывают психологическое давление. Неудивительно, что подобные скоропалительные и умозрительные выводы приводят как минимум к потере объективности.

7. ***Масштаб.***

В этом месте экспертизы необходимо определить, насколько "размыт" МОД географически. Каков его масштаб? Будет ли идти речь о точечной локализации дохода, например, для случая организации ломбарда, или механизм предполагает разброс в пределах всей страны, как это имеет место для газеты бесплатных рекламных объявлений.

В последнем случае винтики МОД рассредоточены, что неизменно приведет к росту накладных расходов и может способствовать различным негативным проектным тенденциям, таким, как утрата централизованного управления, финансовые сложности, слабая контролируемость и проч.

8. ***Легитимность.***

Обычно проверка сводится к выводу о допустимости подобного занятия в рамках принятых фирмой норм и признаваемых ею требований уголовного законодательства. Если предлагается МОД, связанный с импортом табачных изделий, "минуя таможенные формальности", — ваше право решать, стоит ли этим заниматься. Но вы должны знать наверняка, что согласно ст. 194 УК РФ уклонение от уплаты таможенных платежей, взимаемых с организации или физического лица, наказывается штрафом, либо обязательными (принудительными) работами, либо лишением свободы.

9. ***Сложность механики (технологический аспект).***

Почти технический термин, характеризующий сложность внутреннего устройства МОД. Подразумевает наличие в механизме "делания денег" разрозненных переделов.

Оценивается общее количество операций и их содержание. Предмет самого пристального внимания — наличие уникальных операций. С этих позиций понятно, почему сегодня индустриальная бизнес-механика уступает трейдерской.

10. ***Защищенность.***

МОД должен быть устойчив к воздействию агрессивных внешних факторов. Можно построить редкой красоты проект, но малейшее возмущение окружающей среды разрушит его. Поэтому относительная независимость от внешних факторов — качество хорошего механизма дохода. Наличие внутренней защитной механики — признак высокого качества оригинальной идеи.

11. ***Совместимость.***

Проблема совместимости МОД с требованиями окружающей среды — одна из главных. Насколько механика дохода пригодна для существующего объективного окружения?

Большое количество инициативных импортных МОД "сыпятся" на проверке совместимости. Следует предусматривать это до того, как будут затрачены существенные интеллектуальные и имущественные ресурсы на изначально обреченный проект.

12. ***Критерий "Ответ".***

Здесь подразумевается исследование МОД на предмет вероятности, степени и форм возможной ответственности. Для отбраковки несостоятельных проектов достаточным может оказаться исследование негативных черт, свойственных одной лишь генеральной идее. Не стоит забывать, что намерение заработать — это фактически намерение отнять деньги. Последнее может встретить сопротивление или вызвать противодействие.

Предстоит дать ответы на такой вопрос, как "что будет, если..."

Если в плане полулегальных, пограничных и откровенно криминальных проектов ситуация проясняется беседой с адвокатом, "авторитетом" или даже простым перелистыванием УК РФ, то для легальных проектов она может оказаться не столь явной.

13. ***Серверная механика.***

Серверная механика — это система стимулирования продаж, схема организации дистрибуции товара, создание различных управленческих звеньев и т. д. Это могут быть и не очень афишируемые конструкции, например, такие, как организация прикрытия деятельности, легализация или сокрытие дохода, минимизирующие налоговые выплаты. На этапе экспертизы генеральной идеи дохода в обязательном порядке требуется учет серверной механики, так как очень часто серверами оказываются весьма сложные вещи.

Итак, рассмотрено проведение блиц-экспертизы состоятельности главной предпринимательской идеи — дохода планируемого

дела. Даже подобный поверхностный анализ служит хорошим фильтром для отбраковки слабых инициатив.

Кратко сформулируем основные выводы:

1. Надежность проекта увеличивается с ростом автономности.

2. Монопродуктные проекты, специализированные под выпуск ограниченной товарной номенклатуры, опасны.

3. Ориентация на "человеческий фактор" — признак слабости идеи.

4. Признак сильного МОД: место образования прибыли максимально приближено к местам образования ее основной массы.

5. Чем меньше масштаб МОД — тем лучше. Даже если дело разбросано, основная часть прибыли должна централизованно рождаться, а не только аккумулироваться.

6. Можно не уважать закон, но нельзя его не учитывать.

7. Чем проще МОД — тем ближе к деньгам.

8. Зашита МОД — чисто внутреннее свойство идеи доходной механики.

9. Несовместимость МОД видна, если смотреть хорошо.

10. "Ответная" часть МОД должна быть скрупулезно исследована. Если она слабовата, т. е. изобилует всевозможной ответственностью, — проект должен быть если и не отбракован совсем, то хотя бы серьезно доработан.

1.3.4. Маркетинг

Маркетинг в наибольшей мере соответствует технологиям безопасности. Поиск, анализ информации, пресечение инвестиционных провалов — эти основы экономической безопасности в полной мере соответствуют основным характеристикам маркетинга.

Само понятие маркетинга многообразно, простирается от стратегического планирования деятельности до рабочих приемов технологических операций. В принципе весь бизнес и предпринимательство можно свести к проблемам маркетинга: от маркетинга идей до маркетинга реинвестирования прибылей.

Такая размытость и многоаспектность понятия снижает эффективность применения знаний, накопленных в условиях нашей действительности. То, что оказалось пригодным для одного, может быть вредно другому.

Учитывая вышесказанное, введем искусственные ограничения: внимание будет нацелено на главное — проверку рыночной состоятельности генеральной идеи проекта и его вспомогательной серверной механики.

Маркетинговые исследования проводятся сразу же после качественного анализа МОД. Цель работы — убедиться, что предлагаемый механизм образования дохода имеет основания. Это соответствует всей бизнес-практике, где любые провалы сводятся к простой формуле: "товар не нашел сбыта".

В настоящем разделе рассмотрим, как СБ работает над уточнением надежности оценок механизма возможного дохода. "Что", "где" и "как" можно и нужно смотреть и анализировать, применяя специальные методы экономической разведки, для того чтобы избежать провала на старте. Выполнение специального маркетинга, осуществляемое поэтапно, предохранит от ошибок, поможет выработать эффективное, возможно, уникальное, решение.

В качестве основы для демонстрации маркетингового подхода СБ разберем наиболее трудный вариант маркетинга — пионерный проект продвижения нового розничного товара.

Основные элементы маркетингового анализа

При исследовании реальности МОД пионерного проекта проверяется потенциальная готовность рынка к принятию нового продукта. Признаки такой готовности достаточно понятны, непонятным является их недосмотр.

Рыночная ниша

Характеристика, наиболее свойственная проектам продвижения новых товаров. В качестве агрегированного показателя характеризует потенциальную готовность рынка к принятию товара или услуги. Условное западное деление покупателей на всевозможных "первопро-

ходцев", "ранних усыновителей" и т. д., равно как и такие находки маркетинговой мысли, как пресловутая "матрица Бостонской группы" с ее "собаками" и "дойными коровами", представляются малопригодными на таком диком рынке, как наш. Эти подходы не только ничего не предсказывают, но и мало что объясняют из текущих наблюдений.

Ключевые позиции разведки рынка должны иметь совершенно четкие характеристики, позволяющие принимать инвестиционные решения и прогнозировать денежные потоки.

Рассмотрим механику наиболее распространенных ценовых ошибок, приводящих к провалам торговых программ. Каковы причины неправильного выбора цен?

1. ***Недооценка двойственной роли сознания в решении о покупке.***

Ключевой фактор рыночного приживания или отторжения любого товара — баланс между наличием в товаре позитивных и негативных характеристик, отражающихся в сознании покупателя. Поскольку сознание российского покупателя специфично, его нужно прежде изучить, а уже затем определять цены.

Атака на покупателя должна строиться на тех же принципах, что и любое психологическое воздействие. То, что называется "психологией покупателя", можно назвать знаниями, используемыми при воздействии на человека. С этих позиций и проведем дальнейшее рассмотрение маркетинговых проблем.

Каждый товар имеет самые разнообразные наборы характеристик. Рассматривая вещь, щупая ее и пробуя на зуб, потребитель соотносит свои внутренние ожидания с данным предложением — вещью. Вещь несет в себе комплекс потенциального удовлетворения различных потребностей покупателя, своеобразный букет вожделений, но не только. В том же букете можно обнаружить массу неприятных ощущений, непосредственно вызываемых товаром в человеке.

Одним из них, хотя и далеко не главенствующим, как это многим кажется, является цена товара как вполне реальная угроза карману покупателя. Принцип Парето в данном воплощении формулируется следующим образом: небольшая совокупность характе-

ристик товара определяет ядро его потребительских качеств, как хороших, так и плохих. Нормальный человек воспринимает новую вещь именно набором Парето, выражаемым целостным представлением обобщенной совокупности положительных и отрицательных характеристик.

Такое восприятие всплывает в сознании в виде единого и неделимого представления, нередко в виде воображаемой картинки или иного эмоционального ощущения. Причем такие проявления у каждого свои, строго индивидуальные.

Это приводит к первому практическому выводу: насколько точно вы прогнозируете "отклик сознания" покупателя на ваш товар? Одна из высокодоходных (автоматически — повышенно рисковых) стратегий предполагает ориентацию на положительный отклик сознания, при котором покупатель закрывает глаза на цену товара, ориентируясь исключительно на мир своих внутренних ощущений, вызываемых, допустим, внешним видом товара.

"Розовый дым" исправно работает на продажах любых товаров, где продавец сумел найти ключ к сознанию покупателя. Прагматичные рассуждения, свойственные западному покупателю, в области новых товаров россиянам пока не свойственны.

Сознание может породить ощущения, совершенно противоположные ожидаемым, ощущения, которые отталкивают покупателя от предлагаемого товара. Расспросите человека, почему он отвернулся от вашего товара, что заставило его воздержаться от покупки? Вас поразит несоответствие сказанного тому, что вы ожидали услышать, и далеко не всегда в отказе от покупки виновата цена.

Ценовой фактор начинает играть роль только в ситуации амбивалентного выбора, когда вещь воспринимается противоречиво: в ней есть и "за" и "против", причем "против" подкрепляются ценовыми аргументами. Ситуация меняется диаметрально противоположно сразу же после прохождения момента "розового дыма".

Как только в сознании включается ценовой фильтр, россиянин показывает чудеса анализа. Многим бизнесменам кажется вполне

приемлемым установление цены по принципу аналогии: "Все торгуют по 100, мы будем торговать по 95. Люди побегут!" А есть ли ценовые аналогии в сознании покупателя, когда речь идет о принципиально новом товаре?

2. ***Игнорирование степени осознания потребности в новом товаре.***

Из дискуссий по этому вопросу можно сделать предположение, весьма часто высказываемое некоторой частью активных российских предпринимателей: зачем тратиться на маркетинг нового продукта, не имеющего аналогов? Не проще ли попросту завезти его из-за границы или создать своими силами и попробовать продать? Опыт подобных подходов дает однозначный ответ: проще, но, как ни странно, дороже.

Пока в сознании не будет отклика при виде вашего товара, пока его потребительские качества не станут узнаваемы — вряд ли его будут активно раскупать.

Известна наработанная в этой области схема продаж "деньги потом", при которой новый товар предоставляется покупателю на некоторое время в ознакомительное пользование с оплатой, скажем, через три недели или с трехнедельной гарантией возврата платежа, если товар покупателя не устроит.

Это менее рискованные стратегии, чем просто атака на покупателя с товаром наперевес. Исследуйте сознание массового покупателя. Это не так сложно и намного дешевле неоправданных рисков!

Продолжим рассмотрение ценового фактора. Мы подошли к простому, но далеко не очевидному выводу: цена — это стоимость внутренних ощущений или воображаемой картинки. Без привязки к тому, ценой чего она является: товара или сделки, предмета ширпотреба или оборудования. Цена по своей психологической природе двойственна, так как всегда, разглядывая ценник, ваш покупатель прислушивается к своему внутреннему голосу. Как это использовать на практике?

Вспомните облюбованный маркетологами график зависимости раскупаемости товара от цены. При традиционном подходе маркетологи обычно упускают из виду части графика, отражающие два

особенных психологических момента, весьма способных изменить подход к установлению цены.

Суть их в том, что по мере увеличения цены человек на некоторое время перестает реагировать ("зоны молчания"), затем начинает реагировать по той же зависимости, но на более высоком уровне. Таким образом, стартовая цена на новый товар может быть определена исходя из интересов второго, третьего и более высоких уровней. И в этом нет ничего невероятного. До утери "массовости" сбыта еще очень и очень далеко.

Но тут вы получаете обширные возможности позиционирования своего товара для расширения сбыта по более низкой цене. Отметим, что традиционный подход сводится к установлению низкой стартовой цены продвижения товара, при этом планируется, что цена будет поднята после закрепления товара на рынке, и, как правило, как только это происходит, новая цена попадает в "зону молчания" и товар перестает расходиться.

На этом маркетолог-ортодокс останавливается, делая неверный вывод о достижении ценой критического показателя. Маркетолог — сторонник нашего подхода сделает иначе, начав строить ценовую интервенцию с мотивов второго или третьего уровня.

3. ***Неадекватная ценовая политика.***

Изменяя цену на один и тот же продукт, можно добиться разных эффектов сбыта, включая парадоксальный. Парадоксальный эффект выглядит так: низкая цена может отталкивать покупателя, непомерно высокая цена — притягивать. Механика, как мы видели, уходит корнями в преодоление "зоны молчания" и начало реагирования на более высоком уровне.

Другое возможное объяснение может быть связано с рациональной механикой внутренних мотивов покупателя: за низкой ценой товара наш пуганый потребитель начинает подозревать скрытый в товаре подвох, а высокая цена может запустить в русской душе механизм типа "один раз живем!". Такой "розовый дым" миру неизвестен, как убедительно показывают всем "новоруссы", скупающие за рубежом недвижимость и предметы роскоши по баснословно высоким ценам.

Цена товара, отражающая один из самых веских контраргументов покупки, должна рассматриваться одновременно с оценкой потребительских характеристик товара. Это как весы: "хочется" против "можется". И даже законное соответствие еще не гарантирует успеха в отношении нового товара.

Даже проверенная временем ценность и отработанное ценообразование в условиях иноземных рынков еще не только не предопределяют успех товара, но даже не гарантируют его от провала на рынке российском.

4. ***Попадание в "неплатежеспособный" рыночный сегмент.***

Достаточно распространенная ошибка предпринимательства заключается в том, что, планируя продвижение на рынок нового товара, маркетологи или предприниматели без должной серьезности относятся к исследованию платежеспособности потенциальных покупателей — основной действующей силы рыночного сегмента.

Традиции маркетинга, требующие обязательного описания профиля потребителей, включая исследование их доходов, оценку их общего количества, что вливается в такое понятие, как "емкость рынка", в связи с этим весьма понятны.

5. ***Ценовая непластичность.***

Ценовая пластичность, являясь кардинальным моментом ценообразования, как правило, задается если не самим МОД, то его серверной механикой.

Если у вашего товара нет запаса хода в ценовом маневрировании — он обречен на вытеснение. Подобный нюанс, как правило, предопределен внутренним содержанием МОД и схемой реализации проекта. Это значит, что проект слаб изначально. Вам остается только выполнить прогноз развития рыночной ситуации и сравнить последствия с имеющимися возможностями корректировки схемы ценообразования. Что, если рыночная ситуация вынудит вас к снижению цены, а в вашей схеме МОД ценовых люфтов не окажется?

Неписаное, интуитивно нащупанное торговцами "правило 40", относящееся к импортируемому товару, гласит, что в отпускной валютной цене товара должно быть заложено не менее 40% на сбы-

товые издержки. Если не предусматривать этот "резерв", то можно понести еще большие расходы.

Конкуренция

Проект может не выдерживать предлагаемой рынком конкуренции. Чем это быстрее будет установлено — тем лучше.

Даже если на момент проведения маркетинга все представляется относительно безопасным, необходимо исследование тенденций развития рыночной ситуации в данной товарной области.

Требуется оценить рыночные тенденции, прознать намерения и спрогнозировать поведение ближайших конкурентов. В этом деле возможности СБ раскрываются в наиболее яркой и действенной форме.

Ограничения связаны с наличием средств на проведение подобных работ и с некоторыми трудностями объективного плана, такими, например, как невозможность полного выявления всех рыночных фигур.

Для ситуации с новыми товарами дело осложняется еще и тем, что вам неизвестны инициативы миллионов других предпринимателей. Возможно, в то самое время, пока вы строите прогнозы, кто-то из них пакует товар, кто-то устраивает презентации, кто-то уже считает выручку от продаж. Просрочка в три-четыре недели чревата утерей рыночного приоритета.

Бывали случаи, когда совершенно пустые рыночные ниши заполнялись несколькими десятками фирм в течение месяца. Предусмотреть случайное поступление конкурентного товара извне также бывает трудно. Для профилактики подобного прокола хороший эффект дает совмещение внутреннего маркетинга с внешним.

С точки зрения СБ, выяснение рыночной диспозиции приравнивается к рекогносцировке в ходе боевых действий. Вместе с тем, как ни странно, говорить об острой повсеместной конкуренции сегодня не приходится. Места под солнцем хватает всем.

Поэтому рассмотрим только один аспект, представляющий наибольшую опасность со стороны конкурентов. Это обширная

развитая практика конкуренции нерыночными методами, включая допустимость применения к конкуренту мер физического воздействия для вытеснения с рынка.

Острота конкуренции в условиях нашей действительности представляет наиболее опасный маркетинговый фактор. Последствия попадания в условия острой конкуренции могут быть самыми плачевными. Рынок может убить в прямом и переносном смысле.

Не просто плохо, а очень плохо, когда ваш проект затрагивает наиболее агрессивные "горячие" рыночные сегменты, где конкуренция обострена чисто по-российски, без должного понимания этого факта со стороны инициаторов проекта. Такие сегменты общеизвестны и легко обнаруживаются по частоте упоминания связанных с ними трагедий в криминальных разделах массовой печати.

Сбыт

Этот элемент маркетинга относится к серверам МОД. Ограничимся кратким обзором вопросов, связанных с негативными моментами возможных схем дистрибуции, получившими распространение на текущий момент:

1) *дилеры* могут перекинуться к вашим конкурентам со своими дольками рынка или диверсифицироваться, забыв про ваш рынок. Также может наблюдаться дефицит оборотных средств дилеров. Нередки случаи завышения цены по инициативе дилеров, что приводит к утере управления ценовой стратегией;

2) *торговые агенты личной продажи.* Личные продажи — один из самых перспективных и универсальных методов. С ростом накладных расходов, свойственных другим формам торговли, сеть торговых агентов, возможно, в самом ближайшем времени станет наиболее действенным рыночным механизмом распространения не только дорогостоящих товаров, но и самых что ни на есть ширпотребных. Региональные агенты при обеспечении надлежащего стимулирования мобилизуются быстро, эффективность их действий может быть уникальной. К числу их основных недостатков относится высокая текучесть кадров. Приме-

нимость метода ограничена только стоимостью товара, в котором заложено агентское вознаграждение;

3) *собственная торговая сеть* связана с пикообразным всплеском накладных расходов. Если вы привязаны к дорогим рынкам типа столичного, они не только вырастут на порядок, но и станут непредсказуемы. В любой момент могут активизироваться всевозможные сопряженные с делом "отстежные" факторы, от введения новых муниципальных налогов до последствий передела рынка мафиозными структурами;

4) *презентации, выставочная торговля* имеют ограниченный охват, высокие накладные расходы. Кроме того, сказывается психологическая защита потребителя от "массированной контратаки на кошелек", активируемая временным характером акции;

5) *нетрадиционные пути* так же быстро исчезают, как и появляются. Возможно, это связано с подвижностью их основных действующих фигур — инициативной прослойки населения, обделенного имуществом, но не предпринимательской жилкой. Времена, когда каждый второй был "адвайзером гербалайфа", прошли.

Стратегии проникновения на рынок околокриминальными путями также не очень хороши. Достаточно привести пример, как одна фирма пыталась проводить рекламные кампании "левым" распространением программного продукта с "зашитой" в нем рекламой. Пару раз такое сработало, и то в весьма ограниченном рыночном сегменте. И все;

6) *стратегические союзники-ортодоксы* (типа бывших централизованных структур торговли) утрачивают свое значение в качестве единичных потребителей больших товарных партий. Их дистрибутивная мощь падает вместе с обретением самостоятельности подчиненными единицами. Сказываются и пороки чисто внутриорганизационного происхождения;

7) *прямая почтовая доставка* связана с относительно большими невозвратными вложениями в рекламную кампанию на этапе раскрутки. Не имея эффективной обратной связи, вполне может не оправдать возложенных ожиданий, провалив сбыт даже хорошо

распространяемого иными путями товара. Известны случаи массового возврата товаров, ранее заказанных и подлежащих оплате наложенным платежом при получении на почте. В условиях растущей стоимости почтовых услуг теряется экономическая эффективность;

8) *торговля по образцам* связана с трудностями расчетов между покупателем и продавцом, требует товарного запаса, что весьма рискованно. Некоторая подстраховка предполагает торговлю исключительно за валюту, что, как известно, запрещено и к тому же не снимает основного бремени невалютных рисков.

Сформированность рынка

Сформированность рынка является комплексной маркетинговой характеристикой.

Если мы говорим, что в отношении такого-то товара рынок сформирован, то это означает буквально следующее:

1. Известны основные действующие рыночные фигуры и степень остроты рыночной конкуренции между ними.

2. Товар известен потребителю и готов к приему как по осознанию, так и по деньгам целевого рыночного сегмента.

3. Структура цен на рынке сложилась достаточно для уверенного прогнозирования тенденции.

4. Сбыт товара налажен, и имеется достаточный выбор как сбытовых схем, так и лиц, специализирующихся в области торговли данным продуктом.

Из этого списка становится ясным, что весьма немногие товарные группы попадают в категорию сформированного рынка. Во всяком случае, пионерские проекты, связанные с новым товаром или продуктом, его минуют.

Маркетинговые исследования

Почему можно сказать, что разведка и маркетинговые исследования наиболее близки по духу? Потому что принципы планирования и методы проведения маркетинга в условиях российской действительности в полной мере соответствуют методологии сбора информации средствами промышленной разведки.

Планом маркетинга четко должен быть очерчен контингент исследуемых и методология исследований. Здесь вы вольны пробовать варианты на свое усмотрение: от обработки печатных источников до сбора экспертной информации. Комплексный подход наиболее трудоемок, но дает максимально точные результаты. Обычно под маркетингом подразумевают опрос более вширь, нежели вглубь.

В зависимости от выбранного образа действия можно приступать к сбору информации. Для начала используются наиболее простые методы, например, такие, как сбор информации путем телефонного или анкетного опроса необходимого контингента. Эффективнее всего живое общение, исходя из того, что тут можно по ходу дела что-либо менять.

1.3.5. Методы проверки документов

Обмен документами, будь то коммерческое предложение или обширное приглашение к сотрудничеству, устойчиво входит в практику. Обмен устными сообщениями утрачивает свое значение. Даже устоявшиеся партнеры предпочитают обмениваться бумагами.

Бумагам, инициирующим предпринимательскую деятельность, следует уделять больше внимания, чем это делается обычно. Благодаря специальному анализу из них можно получить гораздо больше информации, чем хотели бы предоставить авторы.

Анализ исходного документа складывается из анализа его внешнего вида, упаковки и оформления, способа доставки и исследований содержания и содержательной формы.

По первой позиции следует отметить самую важную деталь — ***проверку реквизитов.***

В любом послании, даже если это всего лишь "рыба", в обязательном порядке должны присутствовать реквизиты фирмы-инициатора. Всем прекрасно известно, что они должны в себя включать. Однако зачем и как это необходимо проверять в обязательном порядке — известно далеко не каждому.

Проверка юридического адреса предохраняет от риска вовлечения в работу с фирмой, относящейся к криминальному миру.

Проверки юридического адреса и банковских реквизитов проводятся путем обращения в орган, уполномоченный на регистрацию субъектов предпринимательской деятельности. Таковыми органами в России являются органы юстиции на местах. Информацию можно также получить в налоговых органах, отделениях Пенсионного фонда РФ, в нотариальных конторах. Вся информация легально доступна.

Юридический адрес может не соответствовать фактическому размещению конторы. Проверьте фирму на предмет "подставки": что за контора находится по указанному адресу? Насколько это надежно? Разыскать владельца арендуемого помещения также труда не составляет.

Можно предложить простой критерий проверки: проверяйте, если стоимость того, о чем идет речь в бумаге, стократно превышает стоимость проверки. Стоимость же рядовой подобной проверки составляет 100–150 долл.

Анализ текста

Используются два основных метода — контентный и морфологический. Один из них позволяет исследовать смысловое содержание послания, второй — внешнюю форму. Оба вместе вскрывают психологические характеристики автора.

Оба они просты, доступны и дают неплохие практические результаты, пригодны не только для анализа текста, но и для исследований речи. Оба метода базируются на нескольких психологических постулатах:

1. Каждый человек составляет бумагу сугубо индивидуально, привнося в нее черты собственного прошлого опыта. То есть потенциально любой текст несет информацию о прошлом автора, что неплохо для получения выводов об опытности, профессиональном и общеобразовательном уровне.

2. При составлении любого текста человек проецирует себя самого на то, что пишет, и это отражает его текущее состояние. Авторский текст всегда персонифицирован. То есть в нем присутствует потенциальная информация о личности автора, включая те позиции структуры личности, которые могут быть связаны с возможным риском для дела.

Обобщенно говоря, личность не скроешь. Чтобы убедиться в этом, достаточно понаблюдать хотя бы за тем, как по-разному составляются тексты самых обыденных справок и сообщений.

Контентный и морфологический методы анализа текста позволяют получить некоторую информацию об авторе и его состоянии в момент написания текста, причем вышесказанное одинаково пригодно как для работы с индивидуальным автором, так и для анализа текстов корпоративных авторов. В случае коллективного творчества можно говорить даже о еще больших возможностях диагностики негативных качеств коллектива.

Итак, чем нетипичнее послание — тем больше информации об авторе можно получить, анализируя текст предлагаемыми методами, так как точность методов и информативность анализа повышаются по мере отклонения послания от шаблонов и нормативных требований делового общения.

Максимум эффекта достигается при анализе корреспонденции личного характера.

Следует оговориться: результаты анализа имеют предположительные и вероятностные черты и носят скорее косвенный, вспомогательный характер. Методы непригодны для анализа формализованных посланий вроде типовых форм и бланков.

Кроме того, сами методы представляют собой весьма обширную область специальных знаний, и нереально изложить их в рамках настоящего раздела полностью. Здесь даны только обобщенные принципы, раскрывающие общий подход. Не следует по ним делать глобальные выводы, пытаться строить точные и далеко идущие прогнозы развития ситуации и делового поведения объекта.

Технология анализа сводится к следующему:

1. Фиксируются точки внимания и выделяются компоненты текста, подлежащие исследованию.

2. Диагностируется каждый компонент на предмет выявления того или иного психологического фактора.

3. По каждому отдельному диагнозу строятся частные предположения об объекте.

4. Синтезируется общее итоговое заключение.

Основные объекты внимания:

• общая приверженность автора текста к нормативным образцам и шаблонам;

• информационный стиль письма;

• литературный стиль: витиеватость — сухость, водянистость, канва послания, уходы мысли в сторону и т. д.;

• технологический стиль составления текста, общая схема построения письма (был ли план письма или перед вами импровизация);

• построение отдельных фраз: синтаксис и пунктуация;

• лексика и фразеология: вес различных компонентов (жаргонизмы, профессионализмы, сленг, термины, степень и обоснованность употребления стандартных и авторских оборотов);

• частота употребления слов, расставленные акценты;

• эмоциональное наполнение послания.

Как уже говорилось, авторский текст несет очень много потенциальной информации. Если вы имеете дело с обширной корреспонденцией — возможности расширяются безгранично. Можно составить полный психологический портрет личности и соответствующей фирмы. Ограничимся рассмотрением тех материалов, которые реально могут попасть в ваши руки, и соответствующих им диагнозов — негативных моментов чужой деятельности.

1. ***Профессиональная компетентность автора.***

Здесь требуется не только понять изложение сути вопроса, но и оценить, насколько она профессионально представлена. Следует уделить особое внимание изъянам профессионализма. Иногда даже в самой рядовой бумаге можно увидеть "прокол" пишущего.

Например, если вам поступает предложение такого рода: *"Уважаемые господа, фирма такая-то заинтересована в поставке товара..."* — и далее следует спецификация товара, то можно предположить, что перед вами не искушенный в торговых сделках партнер. Непонятно, что он хочет — продать или купить. Безграмотное предложение характеризует такую же, если не худшую, деятельность.

При кажущейся нелепости подобных примеров-казусов великое множество, и почти всегда за ними стоят всеядные фирмы-посредники: все — обо всем и ничего о конкретном деле.

Приверженность автора к нормативным образцам и шаблонам может также указать на уровень компетентности автора. Какие материалы были использованы, как автор счел возможным их использовать — все это отражает его профессиональный опыт.

Например, при упоминании цены, скажем, в 100 долл. вам может встретиться написание "100 $". Если автор убеждает, что успешно и продолжительно работает на внешнем рынке — это сомнительно. Работать с инофирмами и не перенять их традиции навряд ли возможно. Обычно указывается так: "$ 100".

С другой стороны, некоторые инициаторы продолжают составлять бумаги нарочито "по-совковому", полагая, что такие бумаги быстрее проходят. На это есть основания.

Наблюдения за работой отдела маркетинга одного крупного завода показали парадоксальный факт: действительно, быстрее всего принимались к исполнению не красиво оформленные "современные" бумаги, а писанные на плохих машинках с ошибками и помарками. Работники отдела утверждали, что именно за такими посланиями стоят реальные заказы.

Скорее всего, выбор формы должен соответствовать ситуации. Плохо, когда видно несоответствие.

Прекрасно, когда бумага обширная, выходит за рамки стереотипов и предоставляет простор для творчества. Например, в бизнес-плане, пояснительной записке, описании проекта можно увидеть профессионализм не только единичных авторов, но и соответствующих служб фирмы-инициатора.

Достаточно указать, что любой стоящий инициативный инвестиционный проект готовится группой специалистов предприятия — объекта возможного инвестирования. Каждый член группы вносит что-то свое, отражая особенности компетенции представляемой им службы. В противном случае соло-проект от организации, писанный каким-нибудь юрисконсультом, характеризует факт несерьезности подхода предприятия в целом.

2. ***Мотив деятельности автора.***

Ответ кроется прежде всего в том, кто и с чем стоит за бумагой. Именно личность инициатора отражается в его подходе к делу. Смысл главной идеи автора просматривается в тексте буквально воочию, причем это касается не только масштабных текстов, но иногда и простенькой бумажки. Например, если вас извещают о намерении прикупить товар такой-то и допускают, скажем, ошибку в наименовании номенклатуры или лишнюю цифру в ГОСТе — навряд ли намерения серьезны и люди компетентны.

Важна и подпись. Если бумага подписана непосредственным руководителем, подразумевается, что он находится в курсе событий. Предпочтение отдается именно таким текстам. Чем ближе подпись к лицу, принимающему решения, тем информативнее текст и объективнее послание.

3. ***Независимость инициаторов.***

Диагностируется по независимости суждений. Наличие подобных наблюдений в тексте говорит о яркой индивидуальности автора. Проверяя кандидатов в партнеры, попросите их составить бумагу достаточно произвольного содержания и посмотрите, как проявится личностное "Я". Качественными признаками могут служить фразеология, речевые обороты и личные обращения.

Предпочтение отдается конструкциям типа "*я считаю...*" вместо традиционного "*мы считаем*". Но будьте внимательны к таким фразам. Их анализ может дать многое. Например, чрезмерное употребление того или иного оборота может указывать на трансформированную самооценку и возможный эгоцентризм или скрытую трусость и нерешительность автора.

4. ***Амбициозность автора.***

Лексика часто выдает амбиции, такие, как стремление к принадлежности к определенному статусу или социальной группе. Например, если в тексте обнаруживаются расхождения между модными ныне экономическими терминами и содержанием, вкладываемым в них автором, можно предположить, что автор в своем стремлении произвести впечатление переусердствовал и пропустил подобный прокол при проверке написанного. Быть

может, он совершенно запутался в своих амбициях. Это говорит о том, что потенциально он может стать объектом манипулирования.

5. ***Скупость.***

Если текст и размещение послания сжаты, слог послания сух и лаконичен, подпись свободна от всевозможных оборотов типа "искренне ваш", "с уважением" и т. д., — автору приписывается возможная скупость.

6. ***Эмоциональное состояние автора.***

Нахождение в тексте следов авторских эмоций позволяет делать вывод о типе темперамента. Это может отражаться во всех анализируемых параметрах текста (стиль письма, включая ритм, построение фраз, расположение отдельных фрагментов текста, выделение абзацев, красных строк, внешнее оформление, отступы полей). Текст может изобиловать прилагательными, в точности соответствующими эмоциональному фону автора.

Например, в деловых письмах, информирующих о некачественной поставке товара, сравните эмоции двух разных людей: "*...вы отнеслись к делу безобразно*" и "*мы считаем, что допущенная вами небрежность...*" Нервозность первого и выдержка и корректность второго отражают не только свойства темперамента и качество эмоций, но и разный подход к делу.

7. ***Диагностика возможных дефектов психики.***

Как распознать внутренние дефекты сознания человека, которые могут сказаться на его деловых качествах? Если текст пестрит выспренними, вычурными фразами, если используются глобальные термины и выражения типа "*развитие России*", "*общечеловеческие гуманные ценности*", "*установление добрососедских отношений между нашими странами*" и т. п., — что-то неладно в мировосприятии автора. С другой стороны, дефекты сознания могут проявляться и в приблатненном слоге послания, особенно если речь идет о солидных суммах.

8. ***Особенности мыслительного аппарата.***

Письмо отражает не только доминирующий тип мышления, но и такие структурные элементы мыслительного аппарата, как под-

верженность стереотипам, оригинальность, логичность, самоконтроль и дисциплина мышления, волевое начало. Обычная экспресс-диагностика, без обращения к специалисту, оперирует такими качествами послания, как "собранность — пространность", "размытость — четкость понятий", "витиеватость — сухость стиля письма" и т. д.

Отдельно анализируется аргументация послания. Пороки мышления диагностируются по информативности послания, лексике, по структуре построения всего текста и частоте употребления отдельных текстовых элементов (словосочетаний, слов, фраз).

9. ***Деловая и общая культура, уровень образования.***

Наиболее приближенные к деловым качествам характеристики автора. Их диагностика не вызывает трудностей. Единственное, что хотелось бы отметить — стойкую недооценку этих несложных и высокоинформативных показателей при прочтении письма.

Прочие деловые качества также можно увидеть уже в первом послании. Например, человек дела строит фразы коротко, начиная с глагольных форм — описания действия.

10. ***Гипертрофированная профессиональная самооценка.***

Следует из общего духа письма. Иногда явно видна в попытках самооценки достижений. Ей присущи использование прилагательных, оборотов речи, символизирующих превосходную степень, чрезмерная частота употребления личного местоимения "я". Все эти наблюдения могут однозначно указывать на гипертрофированную переоценку автором своей профессиональной значимости.

11. ***Манипуляционное и конфликтное поведение.***

Манипуляционная направленность текста может проявляться в различных оборотах, особенно, если послание связано с конфликтом. Апелляция автора к тем или иным моделям разрешения конфликта и выбранная им форма подобной апелляции показывают степень конфликтности автора. Блеф или сдерживаемая мощь, агрессия или миролюбие, стремление воспользоваться вашим положением или готовность к справедливой

компенсации — все это и многое другое видно из послания. И иногда не из текста, а между строк послания.

Выводы и заключения

В результате анализа целесообразно составить ***ориентировку*** о негативных наблюдениях и соответствующих рисках, включая ближайшие перспективы развития ситуации, связанной с настоящим письмом.

Такая ориентировка может включать следующие разделы:

1. ***Целесоответствие предложения проектным целям.***

Сводится к оценке перспективности документа в рамках проводимого проекта. Объем и глубина заключения должны соответствовать свойствам проекта и поставленным задачам. Возможно, достаточно просто отобрать ценные предложения из вороха имеющихся или отследить нужного партнера по заранее заданным параметрам, а возможно, потребуется подвергнуть документ более тонкой обработке.

2. ***Оценка риска.***

Необходимо оценить документ с позиций диагностики возможных рисков. Следует наложить результаты исследований на весь спектр потенциальных проколов: от вероятности агрессии и криминала до личностных дефектов авторов послания. Все, что не понравилось в документе, должно найти соответствующее отражение. На основании диагностики факторов риска документа можно описать возможные негативные пути развития ситуации и предложить соответствующие меры реагирования.

3. ***Психологический портрет инициатора.***

Необходим для учета психологических факторов. Предположительные неделовые наклонности автора должны быть тщательно описаны и привязаны к соответствующему типу негативного поведения. Иногда такой психологический портрет может отбить всякое желание войти в контакт.

Если ничего подозрительного не обнаружено, следует вывод: "Чисто!" Но с поправкой: "Пока что..."

4. ***Рекомендации.***

В итоге такого обзора формируется пакет рекомендаций, как и что необходимо делать далее. Интересен вариант, при котором ре-

комендации могут начаться с определения необходимости глубокой проверки фактов, изложенных в документе.

1.4. Обеспечение безопасности внешней деятельности фирмы

Исключительно важная роль в деятельности службы безопасности фирмы должна отводиться аналитическому подразделению, занимающемуся получением и обработкой информации о фирмах-конкурентах, их слабых и сильных сторонах, деятельности на рынке, о криминально-конкурентных действиях.

Таким аналитическим центром в службе безопасности может быть группа обеспечения безопасности внешней деятельности фирмы.

Цели и задачи такой группы можно обозначить следующим образом:

- контроль за эффективностью функционирования системы экономической безопасности фирмы и выявление фактических возможностей разглашения, утечки и реализации способов несанкционированного доступа к коммерческой тайне (по косвенным признакам, по случаям, имевшим место в других организациях, и т. д.);
- выявление причин и обстоятельств, способствующих утечке ценной информации;
- оценка надежности и эффективности защиты фирмы от внутренних и внешних угроз;
- участие в анализе, разработке и внедрении комплексных экономически и научно обоснованных мер по защите интересов предприятия;
- выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности сотрудников фирмы в ущерб ее безопасности;
- заблаговременное изучение партнеров, клиентов и конкурентов, постоянное отслеживание их действий;
- прогноз вероятных устремлений конкурентов к конкретным сведениям фирмы;

• противодействия промышленному шпионажу конкурентов;

• экономическая разведка — поиск необходимой информации для выработки оптимальных управленческих решений по вопросам стратегии и тактики рыночной деятельности;

• формирование в средствах массовой информации, у партнеров и клиентуры благоприятного мнения о фирме (имиджа), способствующего более глубокому пониманию общественностью специфики фирмы, привлечению внимания к ее деятельности, товарам или услугам в рамках добросовестной конкуренции.

Анализ состояния эффективности экономической безопасности включает:

— изучение и оценку фактического состояния безопасности;

— выявление недостатков и нарушений режима для предупреждения утраты ценного имущества или разглашения коммерческой тайны, причин и условий, их порождающих;

— разработку превентивных мер, направленных на устранение недостатков и предотвращение нарушений.

Аналитические исследования, моделирование вероятных угроз позволяют наметить при необходимости дополнительные меры защиты. При этом важно оценить реальность их выполнения, наличие методического и материального обеспечения, готовность персонала и специалистов службы безопасности их выполнить.

Создание комплексной, всеобъемлющей системы превентивных мер зависит от объективных потребностей и финансовых возможностей фирмы.

Эти объективные потребности определяются следующей совокупностью факторов:

• ожесточенностью конкурентной борьбы на данном конкретном рынке товаров и услуг;

• важностью защиты конкретных ценных сведений;

• реальными возможностями проверки каждого из вероятных каналов утечки закрытой информации (в том числе по конкретным сотрудникам).

Реализация системы превентивных мер требует профессионализма, комплекса специальных знаний и умений, предусматривая:

— использование правил промышленной контрразведки;

— реализацию программы по дезинформации промышленные шпионов и нанявших их конкурентов;

— организацию движения охраняемой информации, не допускающего ее утечку;

— осуществление только руководством фирмы политики взыскания и поощрения применительно к системе превентивных мер: и к сотрудникам, обеспечивающим ее, и к нарушителям.

Одним из основных элементов системы превентивных мер по обеспечению экономической безопасности фирмы является участие аналитиков группы безопасности внешней деятельности в подготовке программы защиты коммерческой тайны и ресурсов фирмы.

Особое внимание группа обеспечения безопасности внешней деятельности должна уделять глубокому, детальному и тщательному анализу деятельности своих конкурентов. Ее аналитическому подразделению совместно со службой маркетинга фирмы необходимо сформировать специальный банк данных для сбора и анализа сведений о конкурентах.

Для этого прежде всего нужен план, который являлся бы программой действий сотрудников группы и отвечал на следующие вопросы: какие сведения следует получить и у кого они концентрируются? Кто и каким образом может получить их с наименьшими затратами? Ожидаются ли трудности в получении желаемых сведений и как их следует преодолевать?

Сотрудники аналитического подразделения при накоплении и анализе сведений должны вести их строгий учет: где, когда и как получена данная информация, кем конкретно и что с ней сделано. Это позволит также своевременно отфильтровать дезинформацию.

Банк данных на каждого из конкурентов (отечественных и зарубежных) должен включать следующие разделы:

• полное название, юридический адрес, телефон, факс;

• фамилии, имена, отчества руководителей, их послужной список и адреса;

• информацию об участии в судебных и иных разбирательствах, залогах имущества, выдержки из газетных и журнальных публикаций и их оценку;

• дату, номер регистрации, по какому адресу и в какой юридической форме это было зафиксировано;

• информацию о практике исполнения платежей;

• банки, с которыми работает фирма, адреса и номера счетов;

• сравнительные характеристики финансового состояния за последние 3 года;

• рассчитанные коэффициенты ликвидности, покрытия, прибыльности вложений, отношение основных средств к инвестициям и др.;

• выдержки из последнего балансового отчета, отчета о прибыли и убытках;

• названия дочерних и родительских компаний, филиалов и отделений;

• характеристику их деятельности: товары и услуги, экспорт-импорт, условия сделок;

• перечисление их партнеров, их характеристики, вероятные связи в криминальной среде;

• коммерческие возможности и финансы;

• организацию работ (особенности технологии, оборудования, ноу-хау и т. д.);

• цели и планы (стратегические и тактические);

• каналы сбыта, особенности работы с клиентурой;

• использование инструментов маркетинга (товарной, ценовой, коммуникационной и рыночной политики);

• стоимость работ, скидки, наценки, финансовые отчеты и др.

Очень важным является сбор информации и анализ научно-технических и коммерческих связей с партнерами и клиентами по следующим направлениям:

— кому и в каких объемах предоставлялась информация о работах предприятия (фирмы);

— как изменились отношения с партнерами и клиентами в зависимости от роста их осведомленности;

— как изменилась рентабельность работы фирмы и ее партнеров;

— какая ценная информация осталась неизвестной партнерам и как она защищается;

— динамика коммерческих связей с клиентами.

Обладание информацией подобного рода по сути своей — один из элементов системы превентивных мер по борьбе с промышленным шпионажем.

За рубежом сведения о клиентах традиционно принято считать не столько секретом фирмы, сколько ее капиталом. Поэтому список клиентов и сопутствующие знания о них должны тоже формироваться в банке данных.

На каждого клиента следует накапливать сведения о его потребностях и желаниях, привычках при заключении сделок, о предоставляемых ему привилегиях. Это могут быть и сведения о требованиях к количеству и качеству товаров и услуг, о том, какие каналы и режимы доставки использовались, какова периодичность поставок, чем они должны дополняться, об оплате и других особенностях контрактов с данным клиентом.

Здесь же сосредотачиваются те сведения, которые определяют прибыльность всех операций с клиентом (ожидаемые объемы сделок, частота поставок, изменение цен и предполагаемые распродажи).

Информация же о наиболее выгодных клиентах конкурента дает шанс "переманить" его клиентуру. Здесь на первый план выступает личностная информация о клиентах, в частности, сведения об их привязанностях, дружеских и иных связях, которые могут повлиять на принятие ими решений о поддержании или прекращении деловых отношений с конкурентами или клиентами.

Таким образом, сбор всей информации о клиентах и конкурентах фирмы должен быть упорядочен самым тщательным об-

разом. Очень важно завести такой порядок, чтобы все продавцы производимых фирмой товаров и услуг представляли в аналитическое подразделение письменные отчеты о конкретных клиентах по каждому факту продаж и вероятные перспективы продаж.

Документация и информация обо всем этом должна быть строго секретной, а сотрудники, работающие с ней, должны строго соблюдать правила обращения с закрытыми сведениями и дать письменные обязательства о неразглашении коммерческой тайны.

Руководство фирмы должно лично направлять и контролировать всю работу с информацией о клиентах и конкурентах.

Рынок, его информационные структуры находятся пока еще в стадии формирования. По этой причине сбор информации, вероятнее всего, может осуществляться:

1) собственными силами службы безопасности, подразделений изучения конъюнктуры, маркетинга и т. д.;

2) получением за плату нужной информации у коммерческих структур (банков, страховых компаний и т. д.);

3) заключением договоров со службами промышленной контрразведки детективных или охранных агентств, со специальными консультационными (консалтинговыми) организациями.

В любом случае этот выбор сделать потребуется потому, что система превентивных мер, обеспечивающая экономическую безопасность фирмы, без исчерпывающей информации о ее клиентах и конкурентах в таких условиях обречена на проигрыш в конкурентной борьбе.

При этом приоритетную роль в системе превентивных мер для достижения конкурентного преимущества может играть экономическая разведка.

В ее задачи входит своевременное добывание информации для выработки руководством фирмы наиболее рациональных управленческих решений, соответствующих складывающейся рыночной обстановке, стратегическим целям и оперативным задачам и позволяющих избежать неудач, полнее и эффективнее реализовать свой интерес в бизнесе, снижая уровень риска.

Специалисты по маркетингу выделяют следующие виды риска внешней среды рынка: экономический риск, политический риск, природный риск и другие, воздействующие в своей динамике на стратегический риск фирмы.

Задача специалистов по сбору и анализу информации заключается в упреждающем выявлении источников внешних угроз экономической безопасности фирмы с тем, чтобы максимально снизить неопределенность стратегического риска.

Такого рода информация должна:

- раскрывать истинные намерения потенциальных и действительных партнеров по отношению к фирме;
- характеризовать сильные и слабые стороны конкурентов;
- помогать оказывать влияние на позицию заинтересованных лиц в ходе деловых переговоров;
- предупреждать о возможном возникновении кризисных ситуаций;
- облегчить контроль за соблюдением партнерами достигнутых ранее договоренностей;
- способствовать выявлению несанкционированных каналов утечки закрытой информации предприятия (фирмы).

Поэтому в выгодном положении будут те фирмы, руководство которых способно лучше и раньше других оценить рыночную ситуацию, вовремя адаптировать свою производственно-сбытовую деятельность к динамично развивающейся рыночной конъюнктуре, правильно оценить реальные отношения с партнерами и конкурентами с учетом внешних и внутренних факторов в своих интересах для повышения эффективности функционирования и конкурентоспособности продукции и услуг.

Недобросовестная конкуренция, как правило, осуществляется в форме промышленного шпионажа, махинаций, обмана потребителей, фальсификации продукции конкурентов и других действий, в зависимости от обстоятельств.

Оценив конъюнктурную ситуацию на рынке, отношения между производителями, можно определить характер отношений и возможные конкурентные действия. Поэтому, если определить типовые ситуации отношений и описать их определен-

ными характеристиками, то оценивать характер отношений между субъектами рынка можно на некотором формальном, качественном уровне в виде **моделей конкурентов**.

Разработка такой модели является достаточно сложной задачей, но необходимость ее очевидна. Предсказание хотя бы на формальном уровне поведения конкурента необходимо как для принятия организационно-управленческих решений, так и для осуществления защитных мероприятий, обеспечивающих экономическую безопасность фирмы с учетом рыночных тенденций. Не выяснив возможностей конкурентов, нельзя определить экономическую и технологическую целесообразность мер защиты.

В основу разработки модели конкурента может быть положено следующее:

- устремления конкурента, направленные на добывание информации о фирме, ее продукции, коммерческих связях, маркетинге и т. п.;
- прямые и потенциальные возможности по "перехвату" интересующей его информации;
- макроэкономическая среда рынка (внешние параметры).

Если главной целью конкурента является получение сведений, составляющих коммерческую тайну, то для достижения этой цели он будет собирать о фирме любую информацию: о ее связях с другими фирмами, потребителями, о работниках (в первую очередь о ведущих специалистах, их интересах, слабых и сильных сторонах их характеров). Наличие такой косвенной информации о фирме поможет имеющему соответствующие цели конкуренту ближе подойти к интересующей его информации. Конечно, возможны и другие, конкретные устремления.

Для реализации своих целей конкурент должен обладать соответствующими возможностями, которые обязательно следует учесть при разработке мер защиты информации.

Необходимо помнить, что возможности конкурента напрямую связаны с недоработками или нарушениями в обеспечении защиты информации: учета и хранения документов, изделий, защиты ра-

бочих мест исполнителей и технологических процессов изготовления продукции, рабочих помещений и офисов, средств связи, множительной техники, стационарных и мобильных ПК.

Наиболее реальными возможностями конкурента следует считать:

- внедрение в штат фирмы;
- использование средств подслушивания и записи речевой информации;
- визуально-оптические наблюдения за местами проведения работ и совещаний;
- использование подкупа и шантажа сотрудников фирмы на основе изучения их характеров, привычек, материальных и моральных проблем;
- использование открытых каналов, научных отчетов в журналах, публикаций и т. д.

Поэтому очень важна профилактическая работа по анализу документации для выявления сведений, которые в совокупности или отдельно составляют ресурс идей, не являющихся общедоступными или доступными посторонним, которые могут использовать их в коммерческих целях.

Этот анализ должен показать:

— где и как возникают идеи, специфические технологии, способные стать основным ресурсом идей фирмы;

— на каких информационных носителях проявлены или могут проявиться идеи, технологии, технико-экономические параметры;

— как ранжированы сведения и как осуществляется их защита, какие конкретные идеи стали общедоступными.

Одним из важнейших объектов, интересующих конкурента, являются специалисты, допущенные к основным идеям, работам и продукции фирмы. Опыт работы, знания, талант представляют основную ценность специалиста, и чем выше его осведомленность, тем значительнее к нему интерес конкурента и тем важнее обеспечение его безопасности.

Служба безопасности должна проводить планомерное изучение возможной осведомленности сотрудников и вероятного кон-

курента о работах своей фирмы. Во внимание принимается проявление интереса конкурента, изучается зависимость его осведомленности от деятельности отдельных сотрудников фирмы.

При проведении анализа возможной осведомленности необходимо учитывать следующие факторы:

1. Опасный момент утечки информации может возникнуть на открытых рекламных и торговых мероприятиях или публичных выступлениях (имеются в виду различные презентации, выставки, торги, симпозиумы и др.).

Участие специалистов в этих мероприятиях связано с консультациями, докладами, ответами на вопросы, не исключены также различные дискуссии. В этих ситуациях, задавая заведомо продуманные вопросы, конкуренты могут умышленно провоцировать специалиста на дополнительные разъяснения. Специалисты предприятия должны иметь четкое представление о границах открытого использования информации.

В подобные ситуации часто попадают сотрудники отдела сбыта, менеджеры и другие специалисты, занятые в деловых переговорах. Конкуренты часто задают им вопросы о продукции и ее свойствах, об эксплуатационных возможностях и конструктивных особенностях новых изделий. Эта информация может быть ключевой в конкурентной борьбе.

2. Переход специалистов в другие организации и связанная с этим "утечка мозгов" и ценных идей представляют прямую утрату ценной информации. Служба безопасности призвана применять меры к неразглашению коммерческой тайны и созданию условий для смягчения возможного ущерба в случае использования материалов фирмы бывшими сотрудниками.

3. Дополнительные возможности по "изучению" работ и продукции фирмы возникают у конкурентов в результате командировок специалистов, а также при проведении совместных разработок. При этом должны быть предусмотрены специальные защитные меры. Общение с сотрудниками, посещение рабочих мест, изучение производства и продукции — все это во многом определяет возможности получения исходной (начальной) информации. В этих случаях служба безопасности рекомендует

ограничение приема командированных за счет установления приемных дней. Прием осуществляется в специально выделенных помещениях, экскурсии организуются по специальному маршруту с учетом заранее разработанных мер безопасности.

4. В местах отдыха, спортивных или общественных мероприятий, в которых участвуют сотрудники фирмы, может происходить обмен последними новостями из всех сфер деятельности.

5. Конкурент может использовать способ, получивший в американской практике название "обратный инжиниринг", — разбор изделия (прибора, станка и другой продукции) на составные части или конструктивные элементы с целью изучения устройства, технологии сборки и повторения в своих работах последних достижений.

При изучении осведомленности своих сотрудников и вероятных конкурентов используется принцип сравнения их фактической информированности с той совокупностью ценных сведений, которые приведены в специальном перечне сведений, охраняемых как коммерческая тайна фирмы.

Фактическую информацию можно получить при сборе производственных данных о работах специалиста и выполненных им заказах с учетом используемых материалов, на основании выпущенных отчетов и других документов. Эти данные можно получить от самого специалиста, его сотрудников или непосредственного руководителя работ.

Такой анализ позволяет оценить эффективность действующего на фирме разграничения доступа к информации по различным направлениям работы.

В частности, выявляется, насколько близко специалист знаком со сведениями стратегического, производственного и оперативного назначения. При этом определяется доступность информации сотрудникам и посторонним лицам. Полученная характеристика осведомленности специалиста может помочь в критических ситуациях определить источник утечки информации.

Изучая рынок и конкурирующую продукцию, можно обратить внимание на ее схожесть с продукцией фирмы или короткий срок

разработки конкурентом аналога продукции. В других случаях можно нащупать подход конкурента к коммерческой тайне из его открытых публикаций или рекламных проспектов на новые виды товаров.

Такая аналитическая работа службы безопасности по устранению доступа конкурентов к секретам и некоторым объектам фирмы, а также учет возможных каналов утечки важных для конкурентов сведений является основой разработки превентивных мер. Профилактика и разоблачение применяемых конкурентами методов и приемов промышленного шпионажа могут быть полезными в экономической разведке и при уточнении модели конкурента.

Каналы, по которым группа обеспечения внешней деятельности может получить информацию о конкурентах и клиентах, конкуренты могут использовать в своих целях.

В частности, они могут использовать следующее:

- публикации в открытой печати, передачи по радио и телевидению, отчеты в отраслевых и специальных журналах;
- сведения и данные, публично опубликованные бывшими сотрудниками фирмы;
- обзоры рынков и доклады экспертов-консультантов;
- финансовые отчеты;
- выставки, ярмарки и презентации, устраиваемые фирмой;
- издаваемые фирмой брошюры, печатную рекламу (проспекты, буклеты и т. д.);
- анализ изделий фирмы, в том числе и "обратный инжиниринг";
- отчеты посредников и закупочных отделов;
- переманивание специалистов и заполнение ими специальных вопросников;
- беседы со специалистами фирмы на научных мероприятиях и форумах;
- притворные предложения работы с целью выведывания у них необходимой информации;
- проникновение в базы данных;

• непосредственные тайные наблюдения и подслушивание, засылку агентов, использование профессиональных шпионов, похищение документов, планов и т. д.;

• посягательства на собственность фирмы или ее сотрудников;

• разного рода давление, шантаж, подкуп сотрудников.

Постоянная работа с персоналом и особенно при приеме на работу — важная функция службы безопасности и ее группы внешнего обеспечения.

Интересы охраны секретов фирмы в подавляющем числе случаев находятся в трудноразрешимом противоречии с личными амбициями, самолюбием, академической независимостью сотрудников фирмы, желающих профессионально самоутверждаться в ученом мире, среди своих коллег, в общественном или групповом мнении.

Достаточно сложен для разрешения конфликт между стремлением сохранить коммерческую тайну фирмы и желанием использовать в рекламных целях некоторые наиболее впечатляющие данные из строго охраняемой информации, особенно те из них, которые, несомненно, помогли бы расширить сбыт производимых товаров и услуг.

Сотрудник службы безопасности, осуществляющий цензуру открытых публикаций рекламного, научного и популяризаторского характера, готовящихся персоналом фирмы или по ее заказам, должен руководствоваться простым, но достаточно эффективным правилом.

Суть его в том, чтобы в максимально возможной степени раздробить, разобщить во времени, в пространстве и по авторам ту строго охраняемую коммерческую информацию, без которой невозможно опубликование этих работ.

Некоторые руководители фирм считают, что при решении деловых вопросов нет необходимости отвлекаться на такие "мелочи", как установление доверительных отношений со своими партнерами (клиентами), изучение и учет личностных качеств руководства, манер, привычек, их поведения. Однако практика показывает, что чем лучше известен партнер, тем эффективнее проходят разного

рода переговоры и тем безопаснее будет экономическое сотрудничество.

Прежде чем приступить к деловым переговорам, следует выяснить цель, которую преследует партнер, какие способы ее достижения он применит. Это позволит более правильно выбрать стратегию поведения на переговорах, найти аргументы для его убеждения и т. п.

Если партнер преследует цель достигнуть положительного для него результата в ущерб экономическим или другим интересам фирмы, надо попытаться убедить его в том, что такая стратегия может привести к обоюдному проигрышу или, во всяком случае, сведет на нет его попытки получить одностороннюю выгоду.

Для заключения при деловых переговорах выгодных сделок, реализации товаров конкурирующие стороны стремятся заполучить сведения, позволяющие успешно осуществлять производственно-коммерческие операции, получать максимальную прибыль.

Это обусловливает необходимость строгого обеспечения информационно-экономической безопасности, введения специального порядка проведения таких переговоров для предотвращения утечки ценных сведений.

Особое место защита коммерческой тайны должна занимать в расширяющейся внешнеэкономической деятельности фирм. Внешние контакты связаны с трудностями и риском, поскольку некомпетентные действия на зарубежных рынках могут привести к большим потерям.

В зарубежной практике в основе возникновения, развития и дальнейшего совершенствования такого явления, как экономическая разведка, лежит стремление к обеспечению конкурентных преимуществ — либо национальных, либо корпоративных. Причем концепцией экономической разведки охватывается большая совокупность легальных и нелегальных действий по сравнению с теми, что обозначаются терминами "слежение", "защита собственности конкурента" и "влияние".

Поэтому экономическая разведка на этом уровне включает стратегические и тактические планы, определяющие характер отдельных ее видов и гарантирующие их успех.

В ее сфере находятся также:

- сложная международная игра под названием "сотрудничество-конкуренция";
- конфронтация между основными экономическими блоками, перемежающаяся с переговорами;
- национальные интересы различных стран, практически исключающие какой-либо диалог между ними;
- межрегиональная стратегия государств;
- области языкового влияния и этнические группы.

Таким образом, традиционная "окружающая (внешняя) среда" промышленности в настоящее время коренным образом изменилась, а коммерческая практика фирм стала более агрессивной, так как новые условия потребовали нового подхода к информации, тем более что количественный и качественный рост торговли стимулировал и конкуренцию, и рынки. Это подстегивается интернационализацией экономики, сопровождающейся процессами взаимопроникновения и ростом взаимозависимости национальных хозяйств.

Поскольку концепция экономической разведки включает не только знания, но и действия, она чаще всего используется в наступательном плане.

Вот несколько примеров из зарубежной практики:

- проведение через печать "кампаний влияния" с целью противодействия нежелательным официальным мерам;
- систематический анализ продукции и публикаций конкурента или местного законодательства для выявления их слабостей и ошибок в своих интересах;
- легальное овладение полезной информацией путем прямого воздействия на человеческий фактор (очень эффективны в этом отношении беседы с персоналом того или иного предприятия под прикрытием опроса общественного мнения);
- изучение технических возможностей конкурента с помощью "клиента", на самом деле проверяющего все аспекты системы сбыта конкурента и его служб;

• очернение продукции конкурента путем "информирования" потребителей о ее недостатках.

Совершенно ясно, что средства нападения в экономической конфронтации многочисленны, так как овладение промышленной информацией выходит далеко за пределы технологической слежки или овладения только документацией.

Экономическая разведка — оружие, которое нужно по возможности подчинить закону с тем, чтобы ограничить его потенциал открытой в принципе информацией, понимая при этом, что конкурент все равно пойдет на "браконьерство" в промежуточной зоне и будет "осуществлять набеги" на запретную зону, правда, уже чужими руками.

Словом, необходим контроль за растущим потоком информации, полезной субъекту экономики, находящемуся в условиях жесткой и сложной конкуренции.

Фирмы должны иметь структуры, средства, позволяющие использовать открытую информацию со всех уровней принятия решений. У многих из них нет необходимых ресурсов, и поэтому им приходится действовать по-другому: либо более ограниченно, либо объединяясь с другими в различного рода ассоциации, союзы и т. д.

Подобно большому бизнесу, экономическая разведка не знает государственных границ. Нередко похищенные секреты проходят через несколько рук, прежде чем попадают покупателям. Существуют тайные биржи, где продают краденые промышленные секреты: в Японии — по электронике и пластмассам, в Италии — по фармацевтике. "Черные" биржи украденных секретов имеют своих коммивояжеров, которые разъезжают по всему миру.

Такие биржи располагают достоверной информацией о финансовых и торговых возможностях той или иной фирмы, о ее контрактах и дальнейших планах, о том, над чем работают ее лаборатории и какую продукцию она собирается выпустить. Едва подобная информация попадает на рынок, как она сразу же приобретает определенную стоимость и котируется в зависимости от конъюнктуры.

Наиболее активно промышленным шпионажем занимаются транснациональные корпорации (ТНК). Этому способствует и организационная структура ТНК, сочетающая в себе централизм с делегированием части прав менеджерам, возглавляющим зарубежные филиалы корпораций. Это позволило ТНК создать гибкие системы сбора информации от их многочисленных, разбросанных по всему миру филиалов, причем с учетом специфики регионов и даже отдельных стран.

Есть еще один вид экономического шпионажа, широко практикуемый крупными корпорациями в основном в развивающихся странах, который, однако, в силу ряда известных обстоятельств сегодня стал довольно актуальным и для России и стран СНГ.

Речь идет о практике исследования ТНК малодоступных, малозаселенных и лишенных развитой экономической инфраструктуры районов по просьбам правительств и местных властей с целью изучения возможностей привлечения крупного иностранного капитала для освоения природных ресурсов и экономического развития региона в целом.

Результаты исследований подобных районов, как правило, оказываются недостоверными, а именно — резко заниженными. Зная достоверные данные, ТНК выторговывают себе столько льгот, что зачастую государства, чьи природные богатства эксплуатируются, остаются у них в вечных должниках или же получают неадекватный экономический эффект от такого "сотрудничества".

Суммируя вышесказанное, к ***основным принципам экономической разведки*** можно отнести:

- подчиненность задач и целей экономической разведки ключевым национальным экономическим интересам;
- независимость выбора объектов экономической разведки от политических, военных и иных отношений между государствами;
- постоянство в ее ведении;
- дестабилизирующее и иное деструктивное воздействие на экономическую структуру государств и объектов их экономики;

• стимулирование деятельности по экономической разведке со стороны заинтересованных в получении разведывательной информации компаний, финансово-промышленных групп и фирм.

Анализ разведывательно-подрывной деятельности иностранных спецслужб показывает, что объекты экономики стран СНГ попрежнему остаются целью их первоочередных устремлений. Особый интерес для спецслужб представляют сведения, характеризующие состояние и динамику развития нашей экономики, данные о новейших достижениях и открытиях, о развитии приоритетных отраслей промышленности, позволяющих поддерживать на высоком уровне наше оборонное производство.

Спецслужбы ведущих зарубежных стран постоянно ищут новые формы и методы добывания в странах СНГ информации научно-технического и общеэкономического характера.

Неотъемлемой частью экономической разведки стал и промышленный шпионаж, ведущийся негосударственными организациями и частными лицами.

Промышленный шпионаж осуществляется с целью овладения рынками сбыта, подделки товаров, дискредитации или устранения конкурентов, срыва переговоров по контрактам, перепродажи фирменных секретов, шантажа определенных лиц, создания условий для подготовки и проведения террористических и диверсионных акций.

Число частных организаций, специализирующихся на добывании сведений о конкурентах, постоянно растет. Промышленный шпионаж и экономическая разведка являются единственной предпринимательской отраслью, которая не страдает от возникающих периодически кризисов экономики. По мере роста инфляции, усиления конкуренции и социальной напряженности промышленный шпионаж активизируется.

Это необходимо учитывать руководству фирмы при выходе на зарубежные рынки, организации внешнеэкономической деятельности и создании совместных предприятий. Важно располагать объективной информацией, цивилизованно и грамотно проводить

коммерческие сделки, защищая свои ценные секреты от недобросовестной конкуренции, не робеть и не заискивать перед зарубежными партнерами и клиентами.

При идентификации и категоризации сведений, относимых к коммерческой тайне, организации их защиты очень важно учитывать требования (критерии) национальной экономической безопасности государства, чтобы утеря или несвоевременное использование каких-либо ценных открытий, изобретений, ноу-хау и другой интеллектуально-промышленной собственности фирмы не нанесли экономический урон экономике или престижу страны.

Одной из важных функций группы обеспечения безопасности внешней деятельности фирмы является своевременное упреждение жульнических действий иностранных организаций и частных лиц.

2. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

2.1. Обеспечение защиты информационных объектов

2.1.1. Проблема защиты информации

Информация играет особую роль в развитии цивилизации. Владение информационными ресурсами и рациональное их использование создают условия оптимального управления обществом. И напротив, искажение информации, блокирование ее получения, использование недостоверных данных ведут к ошибочным решениям. Одним из главных факторов, обеспечивающих эффективность в управлении различными сферами общественной жизни, является правильное использование информации различного характера.

Темпы прогресса сегодняшнего, а тем более завтрашнего дня в значительной мере зависят от состояния дел в области информационно-вычислительного обслуживания важнейших сфер деятельности — науки, техники, производства и управления. Особенно актуальна проблема использования экономической информации в сфере управления материальным производством, где рост информационного потока находится в квадратичной зависимости от промышленного потенциала страны.

В свою очередь быстрое развитие процессов автоматизации, использование компьютеров во всех сферах современной жизни, помимо несомненных преимуществ, повлекли появление ряда специфичных проблем.

Одна из них — необходимость обеспечения эффективной защиты информации. Исходя из этого, создание правовых норм, зак-

репляющих права и обязанности граждан, коллективов и государства на информацию, а также защита этой информации становятся важнейшим аспектом информационной политики государства.

Защита информации, особенно в экономической сфере, — очень специфический и важный вид деятельности. Достаточно сказать, что в мире средняя величина ущерба от одной банковской кражи с применением электронных средств оценивается в 9 тыс. долл. Ежегодные потери от компьютерных преступлений в США и Западной Европе достигают 140 млрд долл.

По мнению американских специалистов, снятие систем защиты информации с компьютерных сетей приведет к разорению 20% средних компаний в течение нескольких часов, 40% средних и 16% крупных компаний потерпят крах через несколько дней, 33% банков "лопнут" за 2–5 часов, 50 — через 2–3 дня.

Представляют интерес сведения о проблемах защиты информации, приведших к материальным потерям в компаниях США:

- сбои в работе сети (24%);
- ошибки программного обеспечения (14%);
- компьютерные вирусы (12%);
- неисправности в компьютерах (11%);
- хищение данных (7%);
- саботаж (5%);
- несанкционированное внедрение в сеть (4%);
- прочие (23%).

Бурное развитие и распространение компьютерных систем и информационных сетей, обслуживающих банки и биржи, сопровождается ростом правонарушений, связанных с кражами и неправомочным доступом к данным, хранящимся в памяти компьютеров и передаваемым по линиям связи.

Компьютерные преступления происходят сегодня во всех странах мира и распространены во многих областях человеческой деятельности. Они характеризуются высокой скрытностью, сложностью сбора улик по установленным фактам их совершения и сложностью доказательства в суде подобных дел.

Правонарушения в сфере компьютерной информации могут совершаться в форме:

• махинаций путем компьютерного манипулирования системой обработки данных в целях получения финансовой выгоды;

• компьютерного шпионажа и кражи программного обеспечения;

• компьютерных диверсий;

• кражи услуг (времени), неправомерного использования систем обработки данных;

• неправомерного доступа к системам обработки данных и "взламывания" их;

• традиционных преступлений в сфере бизнеса, совершаемых с помощью систем обработки данных.

Совершают компьютерные преступления, как правило, высококвалифицированные системные и банковские программисты, специалисты в области телекоммуникационных систем. Нешуточную грозу информационным ресурсам представляют хакеры и крэкеры, проникающие в компьютерные системы и сети путем взлома программного обеспечения защиты.

Крэкеры, кроме того, могут стереть или изменить данные в информационном банке в соответствии со своими интересами. За последние десятилетия в странах бывшего СССР появилась мощная генерация высокоподготовленных потенциальных хакеров, работавших в организациях и ведомствах, занимавшихся информационным пиратством на государственном уровне для использования полученной с Запада информации в военных и экономических интересах.

Что же крадут хакеры? Потенциальным объектом может служить любая компьютерная информация, способная принести прибыль хакеру или его работодателю.

К данной информации относятся практически все сведения, составляющие коммерческую тайну фирм, начиная от разработок и ноу-хау и заканчивая платежными ведомостями, по кото-

рым легко "вычислить" оборот фирмы, количество сотрудников и т. д.

Особо ценной является информация по банковским сделкам и кредитам, проводимая по электронной почте, а также о сделках на бирже. Большой интерес представляют для хакеров программные продукты, оценивающиеся на современном рынке в тысячи, а то и в миллионы долларов.

Крэкеры — "компьютерные террористы" — занимаются порчей программ или информации с помощью вирусов — специальных программ, обеспечивающих уничтожение информации или сбои в работе системы. Создание "вирусных" программ — дело весьма прибыльное, так как некоторые фирмы-производители используют вирусы для защиты своих программных продуктов от несанкционированного копирования.

Для многих фирм получение информации с помощью внедрения к конкурентам хакера-программиста — дело наиболее простое и прибыльное. Внедрять соперникам спецтехнику, постоянно контролировать их офис на излучение с помощью специальной аппаратуры — дело дорогостоящее и опасное.

К тому же фирма-конкурент при обнаружении технических средств может в ответ затеять игру, давая ложную информацию. Поэтому свой хакер-программист в "стане врага" — наиболее надежный способ борьбы с конкурентами.

Таким образом, все возрастающая опасность компьютерной преступности, прежде всего в финансово-кредитной сфере, определяет важность обеспечения безопасности автоматизированных информационных систем.

2.1.2. Информационная безопасность фирмы

Конечно, в наших условиях степень автоматизации коммерческой деятельности значительно уступает западным стандартам, поскольку большинство расчетных операций дублируется на бумаге, а обмен платежными документами в реальном времени осложнен из-за отсутствия единого механизма межбанковских коммуникаций и соответствующих правовых норм.

С другой стороны, относительная слабость механизмов защиты и отсутствие у нас в стране юридической ответственности за компьютерные преступления стимулируют злоумышленников и способствуют их безнаказанности.

Следует также учесть, что в подавляющем большинстве случаев в фирмах эксплуатируются однотипные стандартные вычислительные средства, которые хорошо задокументированы и в деталях известны профессионалам. Простейшие механизмы защиты таких изделий (если они вообще используются) легко преодолимы.

Под ***безопасностью автоматизированной информационной системы предприятия (АИСП)*** понимается ее защищенность от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, а также от попыток хищения, модификации или разрушения ее компонентов.

Безопасность АИСП достигается обеспечением конфиденциальности обрабатываемой ею информации, а также целостности и доступности компонентов и ресурсов системы.

Конфиденциальность компьютерной информации — это свойство информации быть известной только допущенным и прошедшим проверку (авторизацию) субъектам системы (пользователям, программам, процессам и т. д.).

Целостность компонента (ресурса) системы — свойство компонента (ресурса) быть неизменным (в семантическом смысле) при функционировании системы.

Доступность компонента (ресурса) системы — свойство композита (ресурса) быть доступным для использования авторизованными субъектами системы в любое время.

Безопасность АИСП обеспечивается комплексом технологических и административных мер, применяемых в отношении аппаратных средств, программ, данных и служб с целью обеспечения доступности, целостности и конфиденциальности связанных с компьютерами ресурсов; сюда же относятся и процедуры проверки выполнения системой определенных функций в строгом соответствии их с запланированным порядком работы.

Систему обеспечения безопасности АИСП можно разбить на следующие подсистемы:

1. *Компьютерная безопасность* обеспечивается комплексом технологических и административных мер, применяемых в отношении аппаратных средств компьютера с целью обеспечения доступности, целостности и конфиденциальности связанных с ним ресурсов.

2. *Безопасность данных* достигается защитой данных от неавторизованных, случайных, умышленных или возникших по халатности модификаций, разрушений или разглашения.

3. *Безопасное программное обеспечение* представляет собой общецелевые и прикладные программы и средства, осуществляющие безопасную обработку данных в АИСП и безопасно использующие ресурсы системы.

4. *Безопасность коммуникаций* обеспечивается посредством аутентификации телекоммуникаций за счет принятия мер по предотвращению предоставления неавторизованным лицам ложной информации, которая может быть выдана системой в ответ на телекоммуникационный запрос.

Объектами информационной безопасности в фирме являются:

- информационные ресурсы, содержащие сведения, отнесенные к коммерческой тайне, и конфиденциальную информацию, представленную в виде документированных информационных массивов и баз данных;
- средства и системы информатизации — средства вычислительной и организационной техники, сети и системы, общесистемное и прикладное программное обеспечение, автоматизированные системы управления офисами, системы связи и передачи данных, технические средства сбора, регистрации, передачи, обработки и отображения информации, а также их информативные физические поля.

В современном мире информационные ресурсы стали одним из мощных рычагов экономического развития, играющим важную роль в предпринимательской деятельности. Более того, отсутствие в сфе-

ре отечественного бизнеса эффективных компьютерных и современных информационных технологий существенно тормозит переход на новые формы хозяйствования.

Рыночная экономика диктует свои законы: и большому, и малому бизнесу необходимо информационное обеспечение коммерческой деятельности, необходимы как базы данных общедоступной коммерческой информации о макроэкономической ситуации и тенденциях развития, так и системы для обработки внутрифирменной информации.

В информационных и автоматизированных системах управления фирмой на первый план выступает обеспечение эффективного решения задач маркетингового управления, т. е. задач учета и анализа контрактов и контактов фирмы, поиска бизнес-партнеров, организации рекламных кампаний продвижения товаров, оказания посреднических услуг, разработки стратегии проникновения на рынки и т. п.

2.1.3. Виды угроз информационным объектам

Общая классификация угроз автоматизированной информационной системе объекта выглядит следующим образом:

1. ***Угрозы конфиденциальности данных и программ.***

Реализуются при несанкционированном доступе к данным (например, к сведениям о состоянии счетов клиентов банка), программам или каналам связи. Информация, обрабатываемая на компьютерах или передаваемая по локальным сетям передачи данных, может быть снята через технические каналы утечки. При этом используется аппаратура, осуществляющая анализ электромагнитных излучений, возникающих при работе компьютера.

Такой съем информации представляет собой сложную техническую задачу и требует привлечения квалифицированных специалистов. С помощью приемного устройства, выполненного на базе стандартного телевизора, можно перехватывать информацию, выводимую на экраны дисплеев компьютеров с расстояния в тысячу и более метров. Определенные сведения о работе компьютерной сис-

темы извлекаются даже в том случае, когда ведется наблюдение за процессом обмена сообщениями (трафиком) без доступа к их содержанию.

2. ***Угрозы целостности данных, программ, аппаратуры.***

Целостность данных и программ нарушается при несанкционированном уничтожении, добавлении лишних элементов и модификации записей о состоянии счетов, изменении порядка расположения данных, формировании фальсифицированных платежных документов в ответ на законные запросы, при активной ретрансляции сообщений с их задержкой.

Несанкционированная модификация информации о безопасности системы может привести к несанкционированным действиям (неверной маршрутизации или утрате передаваемых данных) или искажению смысла передаваемых сообщений.

Целостность аппаратуры нарушается при ее повреждении, похищении или незаконном изменении алгоритмов работы.

3. ***Угрозы доступности данных.***

Возникают в том случае, когда объект (пользователь или процесс) не получает доступа к законно выделенным ему службам или ресурсам. Эти угрозы реализуются захватом всех ресурсов, блокированием линий связи несанкционированным объектом в результате передачи по ним своей информации или исключением необходимой системной информации. Они могут привести к ненадежности или плохому качеству обслуживания в системе и, следовательно, потенциально будут влиять на достоверность и своевременность доставки платежных документов.

4. ***Угрозы отказа от выполнения трансакций.***

Возникают в том случае, когда легальный пользователь передает или принимает платежные документы, а потом отрицает это, чтобы снять с себя ответственность.

Оценка уязвимости автоматизированной информационной системы и построение модели воздействий предполагают изучение всех вариантов реализации перечисленных выше угроз и выявления последствий, к которым они приводят.

Виды угроз:

1) обусловленные естественными факторами (стихийные бедствия — пожар, наводнение, ураган, молния и другие причины);

2) обусловленные человеческими факторами:

— пассивные (вызванные деятельностью, носящей случайный, неумышленный характер). Это угрозы, связанные с ошибками процесса подготовки, обработки и передачи информации; с нецеленаправленной "утечкой умов", знаний, информации (например, в связи с миграцией населения, выездом в другие страны для воссоединения с семьей и т. п.);

— активные (обусловленные умышленными, преднамеренными действиями людей). Это угрозы, связанные с передачей, искажением и уничтожением научных открытий, изобретений, секретов производства, новых технологий по корыстным и другим антиобщественным мотивам; просмотром и передачей различной документации, просмотром "мусора"; подслушиванием и передачей служебных и других научно-технических и коммерческих разговоров; с целенаправленной "утечкой умов", знаний, информации (например, в связи с получением другого гражданства по корыстным мотивам);

3) обусловленные человеко-машинными и машинными факторами:

— пассивные. Это угрозы, связанные с ошибками процесса проектирования, разработки и изготовления систем и их компонентов (зданий, сооружений, помещений, компьютеров, средств связи, операционных систем, прикладных программ и др.); с ошибками в работе аппаратуры из-за некачественного ее изготовления; с ошибками процесса подготовки и обработки информации (ошибки программистов и пользователей из-за недостаточной квалификации и некачественного обслуживания, ошибки операторов при подготовке, вводе и выводе данных, корректировке и обработке информации);

— активные. Это угрозы, связанные с несанкционированным доступом к ресурсам автоматизированной информационной системы (внесение технических изменений в средства вычисли-

тельной техники и средства связи; подключение к средствам вычислительной техники, и каналам связи; хищение различных видов носителей информации: описаний, распечаток и других материалов; просмотр вводимых данных, распечаток, просмотр "мусора"); угрозы, реализуемые бесконтактным способом (сбор электромагнитных излучений, перехват сигналов, наводимых в цепях (токопроводящих коммуникациях), визуально-оптические способы добычи информации; подслушивание служебных разговоров и т. п.).

Основными типовыми путями утечки информации и несанкционированного доступа к автоматизированным информационным системам, в том числе через каналы телекоммуникаций, являются:

- перехват электронных излучений;
- принудительное электромагнитное облучение (подсветка) линий связи с целью получения паразитной модуляции несущей;
- применение подслушивающих устройств (закладок);
- дистанционное фотографирование;
- перехват акустических излучений и восстановление текста принтера;
- хищение носителей информации и производственных отходов;
- считывание данных в массивах других пользователей;
- чтение остаточной информации в памяти системы после выполнения санкционированных запросов;
- копирование носителей информации с преодолением мер защиты;
- маскировка под зарегистрированного пользователя;
- мистификация (маскировка под запросы системы);
- незаконное подключение к аппаратуре и линиям связи;
- злоумышленный вывод из строя механизмов защиты;
- использование "программных ловушек".

Возможными каналами преднамеренного несанкционированного доступа к информации при отсутствии защиты в автоматизированной информационной системе могут быть:

— штатные каналы доступа к информации (терминалы пользователей, средства отображения и документирования информации, носители информации, средства загрузки программного обеспечения, внешние каналы связи) при их незаконном использовании;

— технологические пульты и органы управления;

— внутренний монтаж аппаратуры;

— линии связи между аппаратными средствами;

— побочное электромагнитное излучение, несущее информацию;

— побочные наводки на цепях электропитания, заземления аппаратуры, вспомогательных и посторонних коммуникациях, размещенных вблизи компьютерной системы.

Способы воздействия угроз на объекты информационной безопасности подразделяются на информационные, программно-математические, физические, радиоэлектронные и организационно-правовые.

К *информационным способам* относятся:

• нарушение адресности и своевременности информационного обмена, противозаконный сбор и использование информации;

• несанкционированный доступ к информационным ресурсам;

• манипулирование информацией (дезинформация, сокрытие или искажение информации);

• незаконное копирование данных в информационных системах;

• нарушение технологии обработки информации.

Программно-математические способы включают:

• внедрение компьютерных вирусов;

• установку программных и аппаратных закладных устройств;

• уничтожение или модификацию данных в автоматизированных информационных системах.

Физические способы включают:

• уничтожение или разрушение средств обработки информации и связи;

• уничтожение, разрушение или хищение машинных или других оригинальных носителей информации;

• хищение программных или аппаратных ключей и средств криптографической защиты информации;

• воздействие на персонал;

• поставку "зараженных" компонентов автоматизированных информационных систем.

Радиоэлектронными способами являются:

• перехват информации в технических каналах ее возможной утечки;

• внедрение электронных устройств перехвата информации в технические средства и помещения;

• перехват, дешифровка и навязывание ложной информации в сетях передачи данных и линиях связи;

• воздействие на парольно-ключевые системы;

• радиоэлектронное подавление линий связи и систем управления.

Организационно-правовые способы включают:

• невыполнение требований законодательства и задержки в принятии необходимых нормативно-правовых положений в информационной сфере;

• неправомерное ограничение доступа к документам, содержащим важную для граждан и организаций информацию.

5. ***Угрозы безопасности программного обеспечения.*** Обеспечение безопасности автоматизированных информационных систем зависит от безопасности используемого в них программного обеспечения и, в частности, следующих видов программ:

1) обычных программ пользователей;

2) специальных программ, рассчитанных на нарушение безопасности системы;

3) разнообразных системных утилит и коммерческих прикладных программ, которые отличаются высоким профессиональным уровнем разработки и тем не менее могут содержать отдельные недоработки, позволяющие захватчикам атаковать системы.

Программы могут порождать проблемы двух типов: во-первых, могут перехватывать и модифицировать данные в результате действий пользователя, который к этим данным не имеет доступа, и, во-вторых, используя упущения в защите компьютерных систем, могут или обеспечивать доступ к системе пользователям, не имеющим на это права, или блокировать доступ к системе законных пользователей.

Чем выше уровень подготовки программиста, тем более неявными (даже для него) становятся допускаемые им ошибки и тем более тщательно и надежно он способен скрыть умышленные механизмы, разработанные для нарушения безопасности системы.

В основном небезопасность программ состоит в том, что они могут быть использованы как средства получения критичной информации (данных), циркулирующей в системе.

Целью атаки могут быть и сами программы — по следующим причинам:

1. В современном мире программы могут быть товаром, приносящим немалую прибыль, особенно тому, кто первым начнет тиражировать программу в коммерческих целях и оформит авторские права на нее.

2. Программы могут становиться также объектом атаки, имеющей целью модифицировать эти программы некоторым образом, что позволило бы в будущем провести атаку на другие объекты системы. Особенно часто объектом атак такого рода становятся программы, реализующие функции защиты системы.

Рассмотрим несколько типов программ и приемы, которые наиболее часто используются для атак программ и данных. Эти приемы обозначаются единым термином — ***"программные ловушки"***. К ним относятся программные люки, "троянские кони", "логические бомбы", атаки "салями", скрытые каналы, отказы в обслуживании и компьютерные вирусы.

1. *Люки в программах*. Использование люков для проникновения в программу — один из простых и часто используемых способов нарушения безопасности автоматизированных информационных систем.

Люком называется не описанная в документации на программный продукт возможность работы с этим программным продуктом.

Сущность использования люков состоит в том, что при выполнении пользователем некоторых не описанных в документации действий он получает доступ к возможностям и данным, которые в обычных условиях для него закрыты (в частности, выход в привилегированный режим).

Люки чаще всего являются результатом забывчивости разработчиков. В качестве люка может быть использован временный механизм прямого доступа к частям продукта, созданный для облегчения процесса отладки и не удаленный по ее окончании. Люки могут образовываться также в результате часто практикуемой технологии разработки программных продуктов "сверху вниз": в их роли будут выступать оставленные по каким-либо причинам в готовом продукте "заглушки" — группы команд, имитирующие или просто обозначающие место подсоединения будущих подпрограмм.

Наконец, еще одним распространенным источником люков является так называемый "неопределенный ввод" — ввод "бессмысленной" информации, абракадабры в ответ на запросы системы.

Реакция недостаточно хорошо написанной программы на неопределенный ввод может быть в лучшем случае непредсказуемой (когда при повторном вводе той же неверной команды программа реагирует каждый раз по-разному); гораздо хуже, если программа в результате одинакового "неопределенного ввода" выполняет некоторые повторяющиеся действия — это дает возможность потенциальному захватчику планировать свои действия по нарушению безопасности.

"Неопределенный ввод" — частная реализация прерывания. В общем случае захватчик может умышленно пойти на создание в системе некоторой нестандартной ситуации, которая бы позволила ему выполнить необходимые действия. Например, он может искусственно вызвать аварийное завершение программы, работающей в привилегированном режиме, с тем,

чтобы перехватить управление, оставшись в этом привилегированном режиме.

Борьба с возможностью прерывания в конечном счете выливается в необходимость предусмотреть при разработке программ комплекса механизмов, образующих так называемую "защиту от дурака".

Смысл этой защиты состоит в том, чтобы гарантированно отсекать всякую вероятность обработки неопределенного ввода и разного рода нестандартных ситуаций (в частности, ошибок) и тем самым не допускать нарушения безопасности компьютерной системы даже в случае некорректной работы с программой.

Таким образом, люк (или люки) может присутствовать в программе ввиду того, что программист:

а) забыл удалить его;

б) умышленно оставил его в программе для обеспечения тестирования или выполнения оставшейся части отладки;

в) умышленно оставил его в программе в интересах облегчения окончательной сборки конечного программного продукта;

г) умышленно оставил его в программе с тем, чтобы иметь скрытое средство доступа к программе уже после того, как она вошла в состав конечного продукта.

Люк — первый шаг к атаке системы, возможность проникнуть в компьютерную систему в обход механизмов защиты.

2. *"Троянские кони"*. Существуют программы, реализующие, помимо функций, описанных в документации, и некоторые другие, в документации не описанные. Такие программы называются "троянскими конями".

Вероятность обнаружения "троянского коня" тем выше, чем очевиднее результаты его действий (например, удаление файлов или изменение их защиты). Более сложные "троянские кони" могут маскировать следы своей деятельности (например, возвращать защиту файлов в исходное состояние).

3. *"Логические бомбы"*. "Логической бомбой" обычно называют программу или даже участок кода в программе, реализующий некоторую функцию при выполнении определенного условия. Этим

условием может быть, например, наступление определенной даты или обнаружение файла с определенным именем. "Взрываясь", "логическая бомба" реализует функцию, неожиданную и, как правило, нежеланную для пользователя (например, удаляет некоторые данные или разрушает некоторые системные структуры). "Логическая бомба" является одним из излюбленных способов мести программистов компаниям, которые их уволили или чем-либо обидели.

4. *Атака "салями"*. Атака "салями" превратилась в настоящий бич банковских компьютерных систем. В банковских системах ежедневно производятся тысячи операций, связанных с безналичными расчетами, переводами сумм, отчислениями и т. д. При обработке счетов используются целые единицы (рубли, центы), а при исчислении процентов нередко получаются дробные суммы. Обычно величины, превышающие половину рубля (цента), округляются до целого рубля (цента), а величины менее половины рубля (цента) просто отбрасываются.

При атаке "салями" эти несущественные величины не удаляются, а постепенно накапливаются на некоем специальном счете. Как свидетельствует практика, сумма, составленная буквально из ничего, за пару лет эксплуатации "хитрой" программы в среднем по размеру банке может исчисляться тысячами долларов. Атаки "салями" достаточно трудно распознаются, если злоумышленник не начинает накапливать на одном счете большие суммы.

5. *Скрытые каналы*. Под скрытыми каналами подразумеваются программы, передающие информацию лицам, которые в обычных условиях эту информацию получать не должны.

В тех системах, где ведется обработка критичной информации, программист не должен иметь доступа к обрабатываемым программой данным после начала эксплуатации этой программы. Например, банковский программист не должен иметь доступа к именам или счетам вкладчиков и клиентов, как не должен знать порядка обслуживания клиентов.

В процессе отладки программы допускается предоставление разработчику ограниченного объема реальных данных для

проверки работоспособности программы, но предоставление реальных данных после сдачи программы в эксплуатацию не имеет оправдания.

Из факта обладания некоторой служебной информацией можно извлечь немалую выгоду, хотя бы элементарно продав эту информацию (например, список клиентов) конкурирующей фирме. Достаточно квалифицированный программист всегда может найти способ скрытой передачи информации; при этом программа, предназначенная для создания самых безобидных отчетов, может быть немного сложнее, чем того требует задача.

Для скрытой передачи информации можно с успехом использовать различные элементы формата "безобидных" отчетов, например, разную длину строк, пропуски между строками, наличие или отсутствие служебных заголовков, управляемый вывод незначащих цифр в выводимых величинах, количество пробелов или других символов в определенных местах отчета и т. д.

Если захватчик имеет возможность доступа к компьютеру во время работы интересующей его программы, скрытым каналом может стать пересылка критичной информации в специально созданный в оперативной памяти компьютера массив данных.

Скрытые каналы наиболее применимы в ситуациях, когда захватчика интересует даже не содержание информации, а, допустим, факт ее наличия (например, наличие в банке расчетного счета с определенным номером).

6. *Отказ в обслуживании.* Большинство методов нарушения безопасности направлены на то, чтобы получить доступ к данным, не допускаемый системой в нормальных условиях. Однако не менее интересным для захватчиков является доступ к управлению самой компьютерной системой или изменение ее качественных характеристик, например, чтобы получить некоторый ресурс (процессор, устройство ввода-вывода) в монопольное пользование или спровоцировать ситуацию клинча для нескольких процессов.

Это может потребоваться для того, чтобы явно использовать компьютерную систему в своих целях (например, для бесплатного

решения своих задач) либо просто заблокировать систему, сделав ее недоступной другим пользователям. Такой вид нарушения безопасности системы называется "отказом в обслуживании" или "отказом от пользы".

"Отказ в обслуживании" чрезвычайно опасен для систем реального времени — систем, управляющих некоторыми технологическими процессами, осуществляющих различного рода синхронизацию и т. д.

7. *Компьютерные вирусы.* Компьютерные вирусы получили широкое распространение в конце 1980-х гг. и представляют в настоящее время серьезную угрозу для безопасности компьютерных систем. Основную массу вирусов составляют модификации "классических" вирусов и "студенческие" вирусы (крайне примитивные и с большим количеством ошибок), написанные людьми, только что изучившими язык ассемблера. К самым опасным относятся "профессиональные" вирусы — тщательно продуманные и оглаженные программы, созданные профессиональными, нередко очень талантливыми программистами.

Такие вирусы зачастую используют достаточно оригинальные алгоритмы, недокументированные и мало кому известные способы проникновения в системные области (например, "стелс" — технологию, делающую вирус "невидимкой").

Известно много определений компьютерного вируса, наиболее точным можно считать следующее.

Компьютерный вирус — набор команд, который производит и распространяет свои копии в компьютерных системах и (или) компьютерных сетях и преднамеренно выполняет некоторые действия, нежелательные для законных пользователей систем.

Тело вируса может состоять из команд одного или нескольких языков программирования (наиболее распространенный случай), микропрограммных инструкций, управляющих символов и комбинаций в телекоммуникационных сообщениях, различного рода параметров и т. д. Со временем вирус может эволюционировать, распространяя в компьютерных системах набор команд, отличающийся по форме или содержанию от оригинала.

Попадая тем или иным способом в компьютерную систему, вирус копирует себя в различные места памяти системы, а затем (либо одновременно с этим) производит в ней изменения, в лучшем случае не приводящие к катастрофическим последствиям (например, разнообразные видео- и звуковые эффекты), а в худшем — выводящие систему из строя.

Так как вирус самостоятельно обеспечивает свое размножение и распространение, для восстановления работоспособности системы необходимо уничтожить все копии вируса. В противном случае уцелевшие копии снова саморазмножатся и все неприятности повторятся сначала.

Своим названием компьютерные вирусы обязаны определенному сходству с вирусами биологическими:

- способностью к саморазмножению;
- высокой скоростью распространения;
- избирательностью поражаемых систем (каждый вирус поражает только определенные системы или однородные группы систем);
- наличием в большинстве случаев определенного инкубационного периода, в течение которого выполняемые вирусом несанкционированные действия ограничиваются заражением других программ;
- трудностью борьбы с вирусами и т. д.

Компьютерные вирусы являются квинтэссенцией всевозможных методов нарушения безопасности. Одним из самых частых и излюбленных способов распространения вирусов является метод "троянского коня". От "логической бомбы" вирусы отличаются только возможностью размножаться и обеспечивать свой запуск, так что многие вирусы можно считать особой формой "логических бомб".

Для атаки системы вирусы активно используют разного рода люки. Вирусы могут реализовывать самые разнообразные пакости, в том числе и атаку "салями". Кроме того, успех атаки одного вида часто способствует снижению "иммунитета" системы, создает благоприятную среду для успеха атак других видов. Захватчики это знают и активно используют данное обстоятельство.

Разумеется, в чистом виде описанные выше приемы встречаются достаточно редко. Гораздо чаще в ходе атаки используются отдельные элементы разных приемов.

Процесс заражения вирусом программных файлов можно представить следующим образом. В зараженной программе код последней изменен таким образом, чтобы вирус получил управление первым, до начала работы программы-вирусоносителя. При передаче управления вирусу он каким-либо способом находит новую программу и выполняет вставку собственной копии в начало или добавление ее в конец этой, обычно еще не зараженной, программы.

Если вирус дописывается в конец программы, то он корректирует код программы, с тем чтобы получить управление первым. После этого управление передается программе-вирусоносителю, и та нормально выполняет свои функции. Более изощренные вирусы могут для получения управления изменять системные области накопителя (например, сектор каталога), оставляя длину и содержимое заражаемого файла без изменений.

Способы заражения делятся на резидентный и нерезидентный. *Резидентный вирус* при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращение операционной системы к объектам заражения и внедряется в них. Резидентные вирусы постоянно находятся в памяти и остаются активными вплоть до выключения или перезагрузки компьютера.

Нерезидентные вирусы не заражают память компьютера и являются активными ограниченное время. Некоторые вирусы оставляют в оперативной памяти небольшие резидентные программы, которые не распространяют вирус. Такие вирусы тоже считаются нерезидентными.

Программа, зараженная вирусом, может рассматриваться как разновидность "троянских программ", содержащих скрытый модуль, осуществляющий несанкционированные действия. В данном случае скрытым модулем является тело вируса, а одним из несанкционированных действий — заражение других программ.

Помимо заражения, вирус может выполнять и другие несанкционированные действия, от вполне безобидных до крайне разрушительных, включая уничтожение данных на зараженном диске. Выполняемые вирусом несанкционированные действия могут быть обусловлены наступлением определенной даты или определенного количества размножений или сочетанием определенных условий, например, записи зараженной программы на винчестер.

Зараженная компьютерным вирусом программа или ее копии могут передаваться по сети на другие компьютеры. Количество таких зараженных программ может быть значительным и приводить к своего рода "эпидемиям".

Этому также способствует распространенная в нашей стране практика использования одного компьютера несколькими пользователями. Опасность существенно возрастает при наличии винчестера, программы на котором используются всеми пользователями. В этом случае один неквалифицированный или беспечный пользователь может нанести значительный ущерб другим пользователям.

Любой пользователь персонального компьютера должен иметь минимально необходимые знания о вирусах и способах их распространения.

Отсутствие таких знаний может привести к "вирусофобии". Это может быть:

- самоизоляция, при которой пользователи начинают бояться брать и пробовать интересующие их программы, хотя именно такой обмен информацией является основным методом повышения собственной производительности;
- непоколебимая уверенность в том, что любые программные или аппаратные сбои в компьютере — результаты происков компьютерных вирусов;
- признание за вирусами сверхпроникающих способностей. Например, распространено мнение, что для заражения компьютера достаточно, чтобы, к примеру, USB-флеш-накопитель с вирусом оказался в USB-разъеме.

На самом деле вирус может проникнуть в компьютер при загрузке с этой флешки и при запуске выполняемых файлов, находящихся на ней, а при чтении файлов и при просмотре каталога — нет. Разумеется, во избежание случайного выполнения действий, которые могут привести к заражению, операции с подозрительными на вирус носителями информации должен выполнять только специалист.

Следует отметить, что вероятность попасть под разрушительную атаку компьютерного вируса имеет и свою положительную сторону. Пользователи приучаются уделять адекватное внимание созданию архивных копий своих данных, а также методам повышения надежности их хранения.

По среде обитания различают вирусы сетевые, файловые, загрузочные и др.

Сетевые вирусы являются наиболее сложной и наиболее опасной разновидностью компьютерных вирусов. Сетевым вирусом называется саморазмножающаяся и самораспространяющаяся по сети программа, которая, в частности, может переносить с собой "троянских коней" и обычные вирусы. К счастью, два наиболее известных случая создания таких вирусов не связаны с потерей или разрушением данных (вирус "Рождественская елка" и вирус Морриса).

Файловые вирусы внедряются:

- в выполняемые программы — файлы типа EXE и COM (вирус получает управление при запуске зараженной программы);
- в резидентные модули операционной системы и драйверы устройств с расширением SYS (активация вируса происходит при загрузке операционной системы);
- в объектные файлы и библиотеки (с расширением OBJ и LIB), вирус из которых будет встраиваться в написанную пользователем программу при сборке редактором связей LINK.

Загрузочные вирусы заражают загрузочный сектор диска (Boot-сектор) или сектор, содержащий системный загрузчик винчестера (Master Boot Record). Активируются при загрузке с инфицированного накопителя.

К отдельной группе относятся вирусы, располагающиеся в определенных областях накопителей, находящихся вне поля зрения операционной системы. Это могут быть псевдосбойные кластеры, как в случае вируса "Driver-1024 / Dir", отличающегося "невидимостью" и стремительным распространением.

Существуют и сочетания, например, файлово-загрузочные вирусы, заражающие и файлы и загрузочные сектора дисков. Кроме того, по сети могут распространяться вирусы любых типов.

По деструктивным возможностям компьютерные вирусы можно разделить на следующие группы:

1) безвредные, никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);

2) неопасные, влияние которых ограничивается уменьшением свободной памяти и графическими, звуковыми и прочими эффектами;

3) опасные вирусы, которые могут привести к серьезным сбоям в работе компьютера;

4) очень опасные, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти, и даже повредить оборудование.

При этом в большинстве случаев справедливо следующее правило: если вирус демонстрирует изощренный визуальный или звуковой эффект, то скорее всего он не выполняет массированного разрушения данных.

Вирусы первой и второй групп могут принести и пользу: проникая в компьютерную систему, они выявляют ее слабые места, не нанося по-настоящему серьезного ущерба (как в случае с вирусом Морриса).

Наносимый вирусами ущерб может иметь катастрофический характер (например, уничтожение винчестера) в сочетании с длительным "инкубационным периодом", или, наоборот, вирус может достаточно часто наносить мелкие, трудно обнаруживаемые повреждения данных.

Наиболее опасны как раз не катастрофические повреждения винчестера или флешек (при адекватном архивировании это означает максимум потерю одного дня работы), а мелкие, незаметные изменения файлов данных. В частности, известен вирус, который ищет файлы типа DBF и, найдя внутри файла числовое поле, меняет местами две рядом стоящие цифры. Заметить подобное искажение информации удается обычно слишком поздно, что повлечет значительные затраты времени на исправление данных.

Хотя большинство повреждений, наносимых вирусом, относятся к данным, возможны также повреждения оборудования.

Примерами таких действий являются:

- интенсивное использование плохо охлаждаемого элемента конструкции для вывода его из строя или возгорания в результате перегрева;
- повреждение участка люминофора ("выжигание пятна") на монохроматическом мониторе при использовании особенностей схемы управления;
- действия, способствующие ускоренному износу движущихся частей механизмов компьютера (например, головок винчестера).

Склонность компьютерных вирусов к разрушению и искажению информации может быть использована нечистоплотными конкурентами для нанесения значительного ущерба беспечной фирме. Не исключено также появление в будущем и вирусов-"шпионов", перешедших от уничтожения информации к ее похищению по внешним линиям связи, подключенным к компьютеру.

Действия компьютерного вируса ведут чаще всего к отказу от выполнения той или иной функции (например, блокирование загрузки программы с защищенной от записи флешки) или к выполнению функции, не предусмотренной программой (например, форматирование диска, удаление файла и т. д.).

При этом создается впечатление, что происходят программные сбои или ошибки оборудования. Это впечатление усиливает-

ся способностью вируса выдавать ложные сообщения или искусственно вызывать ошибки системы.

Подозрение на появление в компьютерной системе вируса возможно в случае:

- изменения даты создания и длины файла;
- пропажи файлов;
- слишком частых обращений к диску;
- непонятных ошибок;
- "зависания" компьютера;
- самопроизвольной перезагрузки операционной системы;
- существенного замедления работы процессора;
- появления неожиданных графических и звуковых эффектов ("падение" букв, движущийся на экране ромбик, возникновение на экране световых пятен, черных областей, проигрывание мелодии);
- сообщения антивирусных средств.

6. ***Угрозы информации в компьютерных сетях.*** Сети компьютеров имеют много преимуществ перед совокупностью отдельно работающих компьютеров, в их числе можно отметить разделение ресурсов системы, повышение надежности функционирования системы, распределение загрузки среди узлов сети и расширяемость за счет добавления новых узлов.

Вместе с тем при использовании компьютерных сетей возникают серьезные проблемы обеспечения информационной безопасности. Можно отметить следующие из них:

1. *Разделение совместно используемых ресурсов.* В силу совместного использования большого количества ресурсов различными пользователями сети, возможно находящимися на большом расстоянии друг от друга, сильно повышается риск несанкционированного доступа, так как в сети его можно осуществить проще и незаметнее.

2. *Расширение зоны контроля.* Администратор или оператор отдельной системы или подсети должен контролировать деятельность пользователей, находящихся вне пределов его досягаемости.

3. *Комбинация различных программно-аппаратных средств.* Соединение нескольких систем в сеть увеличивает уязвимость всей системы в целом, поскольку каждая информационная система настроена на выполнение своих специфических требований безопасности, которые могут оказаться несовместимыми с требованиями на других системах.

4. *Неизвестный параметр.* Легкая расширяемость сетей ведет к тому, что определить границы сети подчас бывает сложно, так как один и тот же узел может быть доступен для пользователей различных сетей. Более того, для многих из них не всегда можно точно определить, сколько пользователей имеют доступ к определенному узлу сети и кто они.

5. *Множество точек атаки.* В сетях один и тот же набор данных или сообщение могут передаваться через несколько промежуточных узлов, каждый из которых является потенциальным источником угрозы. Кроме того, ко многим современным сетям можно получить доступ с помощью коммутируемых линий связи и модема, что во много раз увеличивает количество возможных точек атаки.

6. *Сложность управления и контроля доступа к системе.* Многие атаки на сеть могут осуществляться без получения физического доступа к определенному узлу — с помощью сети, из удаленных точек.

В этом случае идентификация нарушителя может оказаться ложной. Кроме того, время атаки может оказаться слишком малым для принятия адекватных мер.

С одной стороны, сеть — это единая система с едиными правилами обработки информации, а с другой — совокупность обособленных систем, каждая из которых имеет свои собственные правила обработки информации. Поэтому, с учетом двойственности характера сети, атака на сеть может осуществляться с двух уровней: верхнего и нижнего (возможна и их комбинация).

При верхнем уровне атаки на сеть злоумышленник использует свойства сети для проникновения на другой узел и выполнения определенных несанкционированных действий. При нижнем уровне атаки на сеть злоумышленник использует свойства

сетевых протоколов для нарушения конфиденциальности или целостности отдельных сообщений или потока в целом. Нарушение потока сообщений может привести к утечке информации и даже потере контроля за сетью.

Различают пассивные и активные угрозы нижнего уровня, специфические для сетей.

Пассивные угрозы (нарушение конфиденциальности данных, циркулирующих в сети) — это просмотр и (или) запись данных, передаваемых по линиям связи. К ним относятся:

- просмотр сообщения;
- анализ трафика — злоумышленник может просматривать заголовки пакетов, циркулирующих в сети, и на основе содержащейся в них служебной информации делать заключения об отправителях и получателях пакета и условиях передачи (время отправления, класс сообщения, категория безопасности, длина сообщения, объем трафика и т. д.).

Активные угрозы (нарушение целостности или доступности ресурсов и компонентов сети) — несанкционированное использование устройств, имеющих доступ к сети, для изменения отдельных сообщений или потока сообщений. К ним относятся:

- отказ служб передачи сообщений — злоумышленник может уничтожать или задерживать отдельные сообщения или весь поток сообщений;
- "маскарад" — злоумышленник может присвоить своему узлу или ретранслятору чужой идентификатор и получать или отправлять сообщения от чужого имени;
- внедрение сетевых вирусов — передача по сети тела вируса с его последующей активизацией пользователем удаленного или локального узла;
- модификация потока сообщений — злоумышленник может выборочно уничтожать, модифицировать, задерживать, переупорядочивать и дублировать сообщения, а также вставлять поддельные сообщения.

7. ***Угрозы коммерческой информации.*** В условиях информатизации бизнеса представляют особую опасность такие способы несанкционированного доступа к конфиденциальной информации, как

подслушивание, копирование, подделка, уничтожение, незаконное подключение и перехват информации.

1. *Подслушивание.* Наиболее активно используются следующие способы подслушивания:

• подслушивание разговоров в помещениях или в автомашине с помощью предварительно установленных радиозакладок ("жучков") или магнитофонов;

• подслушивание телефонных переговоров, прослушивание радиотелефонов и радиостанций;

• дистанционный съем информации с различных технических средств за счет их побочных электромагнитных излучений и наводок (перехват).

Существуют и другие методы подслушивания:

• лазерное облучение оконных стекол в помещении, где ведутся конфиденциальные переговоры;

• направленное радиоизлучение, заставляющее "откликнуться и заговорить" деталь в телевизоре, в радиоприемнике, в телефоне или другой технике.

Подобные приемы, правда, требуют специфических условий и реализуются довольно сложной и дорогой специальной техникой.

Для подслушивания используются разнообразные технические средства: микрофоны акустического или контактного восприятия звуковых колебаний, радиомикрофоны (радиозакладки), лазерные средства прослушивания, специальные средства прослушивания телефонных переговоров.

Миниатюрные и субминиатюрные радиопередатчики камуфлируются под различные предметы одежды или мебели и бытовые приборы. Нередко используются и узконаправленные микрофоны — для подслушивания переговоров на расстоянии, на открытом пространстве или в общественных помещениях: баре, ресторане и т. п.

2. *Копирование.* При несанкционированном доступе к конфиденциальной информации копируют документы, содержащие интересующую злоумышленника информацию, технические носители, информацию, обрабатываемую в автоматизированных информационных системах.

Используются следующие способы копирования: светокопирование, фотокопирование, термокопирование, ксерокопирование и электронное копирование.

3. *Подделка.* В условиях конкуренции подделка, модификация и имитация приобретают большие масштабы. Злоумышленники подделывают доверительные документы, позволяющие получить определенную информацию, письма, счета, бухгалтерскую и финансовую документацию, ключи, пропуска, пароли, шифры и т. п.

В автоматизированных информационных системах к подделке относят, в частности, такие злонамеренные действия, как фальсификация (абонент-получатель подделывает полученное сообщение, выдавая его за действительное в своих интересах), маскировка (абонент-отправитель маскируется под другого абонента с целью получения им охраняемых сведений).

4. *Уничтожение.* Особую опасность представляет уничтожение информации в автоматизированных базах данных. Уничтожается информация на магнитных носителях с помощью компактных магнитов и программным путем ("логические бомбы").

Значительное место в преступлениях против автоматизированных информационных систем занимают саботаж, взрывы, разрушения, вывод из строя соединительных кабелей, систем кондиционирования.

5. *Незаконное подключение.* Контактное или бесконтактное подключение к различного рода линиям и проводам с целью несанкционированного доступа к информации, образующейся или передаваемой в них, используется довольно широко, начиная от контактного подключения параллельного телефонного аппарата и кончая строительством мощных подслушивающих пунктов и постов.

Подключение возможно к проводным линиям телефонной и телеграфной связи, линиям передачи данных, соединительным линиям периферийных устройств, фототелеграфным линиям, линиям радиовещания, линиям громкоговорящих систем, к сетям питания и заземления технических средств, к одно- и многопроводным волоконно-оптическим линиям связи.

Разработаны и используются не только контактные способы подключения и их разновидности (например, контактное подключение с компенсацией падения напряжения), но и бесконтактные способы, обнаружить которые достаточно сложно. Бесконтактное подключение может быть реализовано с помощью сосредоточенной индуктивности (кольцевые трансформаторы) и рассредоточенной индуктивности (параллельно проложенные для этой цели провода).

6. *Перехват.* Радиоразведка ведется путем поиска, обнаружения и перехвата открытых, кодированных и засекреченных передач радиостанций и систем связи. Ведется также перехват электромагнитных сигналов, возникающих в электронных средствах за счет самовозбуждения, акустического воздействия, паразитных колебаний, пассивными средствами приема, расположенными, как правило, на достаточно безопасном расстоянии от источника информации.

Из всех устройств электронно-вычислительной техники наиболее уязвимыми с точки зрения перехвата информации являются дисплеи. Во-первых, непрерывная регенерация изображения на экране позволяет реализовывать многократный радиоприем одних и тех же информативных сигналов при перехвате, а это значительно увеличивает диапазон перехвата. Во-вторых, в дисплеях информация на экранах, как правило, представлена в наиболее наглядной и обобщенной форме.

Угрозу безопасности электронной коммерческой информации представляют также "жучки" — специальные миниатюрные (размером с булавочную головку) технические средства, которые могут быть вмонтированы в ПК. Подобный "жучок" ловит и передает электронные информационные сигналы от технического средства, в котором он установлен. Такие сигналы могут быть зафиксированы и декодированы на достаточно большом расстоянии от "жучка".

В конструкциях "жучков" могут применяться различные механизмы, затрудняющие их обнаружение:

- передача накопленной информации дискретными порциями в течение нескольких микросекунд;

• использование в качестве среды распространения своих сигналов сети электропитания того технического устройства, в котором установлен "жучок";

• маскировка радиочастот, используемых в передатчиках "жучков", путем подбора частот, близких к применяемым в радио- и телевизионном вещании;

• использование "скачущей" частоты передачи.

Данные методы маскировки "жучков" делают малоэффективным способ борьбы с ними, основанный на электронном "прочесывании".

Кроме того, перехвату подвержены переговоры, ведущиеся с подвижных средств телефонной связи (радиотелефон); переговоры внутри помещения посредством бесшнуровых систем учрежденческой связи и т. п.

2.1.4. Характеристика средств обеспечения защиты информации

Методы и средства обеспечения информационной безопасности предприятия

Методами обеспечения защиты информации на предприятии являются следующие:

1. *Препятствие* — метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т. п.).

2. *Управление доступом* — метод защиты информации регулированием использования всех ресурсов автоматизированной информационной системы предприятия.

Управление доступом включает следующие функции защиты:

• идентификацию пользователей, персонала и ресурсов информационной системы (присвоение каждому объекту персонального идентификатора);

• аутентификацию (установление подлинности) объекта или субъекта по предъявленному им идентификатору;

• проверку полномочий (проверку соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);

• разрешение и создание условий работы в пределах установленного регламента;

• регистрацию (протоколирование) обращений к защищаемым ресурсам;

• реагирование (сигнализацию, отключение, задержку работ, отказ в запросе) при попытках несанкционированных действий.

3. *Маскировка* — метод защиты информации в автоматизированной информационной системе предприятия путем ее криптографического закрытия (шифрования).

4. *Регламентация* — метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи информации, при которых возможность несанкционированного доступа к ней сводится к минимуму.

5. *Принуждение* — такой метод защиты информации, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

6. *Побуждение* — метод защиты информации, который побуждает пользователей и персонал системы не нарушать установленные правила за счет соблюдения сложившихся моральных и этических норм.

Указанные методы обеспечения информационной безопасности предприятия реализуются на практике применением различных механизмов защиты, для создания которых используются следующие **основные средства защиты данных**: физические, аппаратные, программные, аппаратно-программные, криптографические, организационные, законодательные и морально-этические.

1. ***Физические средства защиты*** предназначены для внешней охраны территории объектов, защиты компонентов автоматизированной информационной системы предприятия и реализуются в виде автономных устройств и систем.

Наряду с традиционными механическими системами при доминирующем участии человека, разрабатываются и внедряются универсальные автоматизированные электронные системы физической защиты, предназначенные для охраны территорий, охраны помещений, организации пропускного режима, организации наблюдения; системы пожарной сигнализации; системы предотвращения хищения носителей.

Элементную базу таких систем составляют различные датчики, сигналы от которых обрабатываются микропроцессорами, электронные интеллектуальные ключи, устройства определения биометрических характеристик человека и т. д.

Для организации охраны оборудования, входящего в состав автоматизированной информационной системы предприятия, и перемещаемых носителей информации (дискет, магнитных лент, распечаток) используются:

- различные замки (механические, с кодовым набором, с управлением от микропроцессора, радиоуправляемые), которые устанавливают на входные двери, ставни, сейфы, шкафы, устройства и блоки системы;
- микровыключатели, фиксирующие открывание или закрывание дверей и окон;
- инерционные датчики, для подключения которых можно использовать осветительную сеть, телефонные провода и проводку телевизионных антенн;
- специальные наклейки из фольги, которые наклеиваются на все документы, приборы, узлы и блоки системы. При любой попытке вынести за пределы помещения предмет с наклейкой специальная установка (аналог детектора металлических объектов), размещенная около выхода, подает сигнал тревоги;
- специальные сейфы и металлические шкафы для установки в них отдельных элементов автоматизированной информационной системы (файл-сервера, принтера и т. п.) и перемещаемых носителей информации.

Для нейтрализации утечки информации по электромагнитным каналам используют экранирующие и поглощающие материалы и изделия.

При этом экранирование рабочих помещений, где установлены компоненты автоматизированной информационной системы, осуществляется путем покрытия стен, пола и потолка металлизированными обоями, токопроводящей эмалью и штукатуркой, проволочными сетками или фольгой, установкой загородок из токопроводящего кирпича, многослойных стальных, алюминиевых или пластмассовых листов.

Для защиты окон применяют металлизированные шторы и стекла с токопроводящим слоем.

Все отверстия закрывают металлической сеткой, соединяемой с шиной заземления или настенной экранировкой. На вентиляционных каналах монтируют предельные магнитные ловушки, препятствующие распространению радиоволн.

Для защиты от наводок на электрические цепи узлов и блоков автоматизированной информационной системы используют:

- экранированный кабель для внутристоечного, внутриблочного, межблочного и наружного монтажа;
- экранированные эластичные соединители (разъемы), сетевые фильтры подавления электромагнитных излучений;
- провода, наконечники, дроссели, конденсаторы и другие помехоподавляющие радио- и электроизделия;
- разделительные диэлектрические вставки на водопроводах, отопительных, газовых и других металлических трубах, разрывающие электромагнитную цепь.

Для контроля электропитания используются электронные отслеживатели — устройства, которые устанавливаются в местах ввода сети переменного напряжения. Если шнур питания перерезан, оборван или перегорел, кодированное послание включает сигнал тревоги или активирует телевизионную камеру для последующей записи событий.

Для обнаружения внедренных "жучков" наиболее эффективным считается рентгеновское обследование. Однако реализация этого метода связана с большими организационными и техническими трудностями.

Применение специальных генераторов шумов для защиты от хищения информации с компьютеров путем съема ее излу-

чений с экранов дисплеев оказывает неблагоприятное воздействие на организм человека, что приводит к быстрому облысению, снижению аппетита, головным болям, тошноте. Именно поэтому они достаточно редко применяются на практике.

2. ***Аппаратные средства защиты данных*** — это различные электронные, электромеханические и другие устройства, непосредственно встроенные в блоки автоматизированной информационной системы или оформленные в виде самостоятельных устройств и сопрягающиеся с этими блоками. Они предназначены для внутренней защиты структурных элементов средств и систем вычислительной техники: терминалов, процессоров, периферийного оборудования, линий связи и т. д.

Основные функции аппаратных средств защиты:

- запрещение несанкционированного (неавторизованного) внешнего доступа (удаленного пользователя, злоумышленника) к работающей автоматизированной информационной системе;
- запрещение несанкционированного внутреннего доступа к отдельным файлам или базам данных информационной системы в результате случайных или умышленных действий обслуживающего персонала;
- защита активных и пассивных (архивных) файлов и баз данных, связанная с необслуживанием или отключением автоматизированной информационной системы;
- защита целостности программного обеспечения.

Эти задачи реализуются аппаратными средствами защиты информации с использованием метода управления доступом (идентификация, аутентификация и проверка полномочий субъектов системы, регистрация и реагирование).

Для работы с особо ценной информацией фирмы — производители компьютеров могут изготавливать индивидуальные диски с уникальными физическими характеристиками, не позволяющими считывать информацию. При этом стоимость компьютера может возрасти в несколько раз.

3. ***Программные средства защиты данных*** предназначены для выполнения логических и интеллектуальных функций защиты и включаются либо в состав программного обеспечения автоматизи-

рованной информационной системы, либо в состав средств, комплексов и систем аппаратуры контроля.

Программные средства защиты информации являются наиболее распространенным видом защиты, обладающим следующими положительными свойствами: универсальностью, гибкостью, простотой реализации, возможностью изменения и развития. Данное обстоятельство делает их одновременно и самыми уязвимыми элементами защиты информационной системы предприятия.

В настоящее время создано большое количество операционных систем, систем управления базами данных, сетевых пакетов и пакетов прикладных программ, включающих разнообразные средства защиты информации.

С помощью программных средств защиты решаются следующие задачи информационной безопасности:

- контроль загрузки и входа в систему с помощью персональных идентификаторов (имя, код, пароль и т. п.);
- разграничение и контроль доступа субъектов к ресурсам и компонентам системы, внешним ресурсам;
- изоляция программ процесса, выполняемого в интересах конкретного субъекта, от других субъектов (обеспечение работы каждого пользователя в индивидуальной среде);
- управление потоками конфиденциальной информации с целью предотвращения записи на носители данных несоответствующего уровня (грифа) секретности;
- защита информации от компьютерных вирусов;
- стирание остаточной конфиденциальной информации в разблокированных после выполнения запросов полях оперативной памяти компьютера;
- стирание остаточной конфиденциальной информации на магнитных дисках, выдача протоколов о результатах стирания;
- обеспечение целостности информации путем введения избыточных данных;
- автоматический контроль за работой пользователей системы на базе результатов протоколирования и подготовка отчетов по данным записей в системном регистрационном журнале.

Борьба против атак, использующих метод повторного использования объектов, заключается в устранении возможности считать остатки информации. Делается это либо полным затиранием остатков информации или заполнением их какой-либо бессмыслицей (в простейшем случае — просто блоком сплошных нулей или единиц), либо — более тонко — путем отказа любому пользователю в возможности прочитать "свободный" блок до тех пор, пока этот пользователь полностью не заполнил его своей собственной информацией.

В настоящее время ряд операционных систем изначально содержит встроенные средства блокировки повторного использования. Для других типов операционных систем существует достаточно много коммерческих программ, не говоря уже о специальных пакетах безопасности, реализующих аналогичные функции.

Применение избыточных данных направлено на предотвращение появления в данных случайных ошибок и выявление неавторизованных модификаций. Это может быть применение контрольных сумм, контроль данных на чет-нечет, помехоустойчивое кодирование и т. д.

Часто практикуется хранение в некотором защищенном месте системы сигнатур важных объектов системы. Например, для файла в качестве сигнатуры может быть использовано сочетание байта защиты файла с его именем, длиной и датой последней модификации. При каждом обращении к файлу или в случае возникновения подозрений текущие характеристики файла сравниваются с эталонными. Расхождение каких-то характеристик свидетельствует о возможной модификации файла.

Контроль автоматизированной информационной системы заключается в выделении, накоплении в едином месте (так называемом следе контроля), защищенном хранении и предоставлении по требованию авторизованного (для выдачи такого требования) пользователя специальных данных о различных типах событий, происходящих в системе и так или иначе влияющих на состояние безопасности системы.

Контроль системы служит для следующих целей:

• для отслеживания текущего состояния безопасности в защищаемой системе, своевременного обнаружения возможности нарушения безопасности и предупреждения об этом лиц, отвечающих за безопасность системы;

• для обеспечения возможности обратной трассировки (по данным контроля) происшедшего нарушения безопасности с целью обнаружения причин данного нарушения и установления степени ответственности причастных к нарушению лиц.

Слежение может быть разного уровня реализации (программное, аппаратное, программно-аппаратное), разного уровня подробности (обращения к физическим портам, адресам памяти, ресурсам, отслеживание логических ресурсов, использования программ, каналов и т. п.).

Отслеживание, сбор и обработка статистических данных не решают задачу активной обороны, но являются очень хорошим диагностическим средством. Обычно средства слежения фиксируют такое количество взаимосвязанных событий, что невозможно скрыть следы проникновения в систему, отключения системы слежения. В лучшем случае удается так исказить данные системы слежения, что они на первый взгляд выглядят корректными.

Но при внимательном, подробном анализе всегда обнаруживаются маленькие шероховатости, неувязки, несогласованность данных. Поэтому сбор статистических данных оказывается основой, вокруг которой концентрируются самые разные способы обнаружения вирусов и проникновений хакеров в систему.

Отношение к статистическим данным должно быть следующим: крупные, кричащие несоответствия скорее всего говорят об ошибках персонала и особенной опасности не представляют; напротив, мелкие расхождения должны становиться предметом самого придирчивого расследования, поскольку они и являются скорее всего свидетельством сознательного проникновения в систему.

В отличие от многопользовательских операционных систем, в MS DOS не предусмотрено встроенных средств для сбора статистических данных. Но уже простейшая статистика, регистрирующая время начала работы, время запуска и время работы различных программ и процедур, дает хорошую основу для анализа работы системы.

Поэтому различные системы отслеживания, сбора статистических данных, особенно специально спроектированные с целью аккуратной фиксации специфически вирусных (или подозрительных, квазивирусных) событий, при всех накладных расходах, которые они порождают, являются важным и полезным средством в борьбе за безопасность компьютерных систем. Особенно важными эти системы оказываются в локальных и глобальных информационных сетях.

4. ***Аппаратно-программные средства защиты информации*** — средства, содержащие в своем составе элементы, реализующие функции защиты информации, в которых программные (микропрограммные) и аппаратные части полностью взаимозависимы и неразделимы.

Данные средства защиты широко используются при реализации биометрических методов аутентификации пользователей автоматизированной информационной системы. На практике используются следующие методы аутентификации: по знаниям, по имуществу, по навыкам и по уникальным параметрам.

В *аутентификации по знаниям* обычно используется механизм паролей — для того, чтобы подтвердить свои права на доступ, достаточно сообщить системе секретный ответ на ее запрос. Преимущества данного метода — простота реализации и дешевизна, недостаток — невысокая надежность. Если злоумышленник каким-либо образом узнал пароль, то система не сможет отличить его от легального пользователя.

При *аутентификации по имуществу* для подтверждения своих прав необходимо предъявить системе некий "ключ" — предмет, уникальный для каждого пользователя и защищенный от подделки (например, магнитную или smart-карту). Преимущество данного метода — относительно невысокая стоимость реализации, недостат-

ки — требование наличия дополнительного оборудования и трудности в управлении масштабными системами защиты на основе этого метода.

В случае *аутентификации по навыкам* необходимо продемонстрировать какие-то умения, недоступные для других пользователей и плохо поддающиеся подделке (например, клавиатурный почерк).

К преимуществам такого метода можно отнести возможность сокрытия процесса аутентификации пользователя (например, он может и не подозревать о том, что в данный момент система проверяет его манеру печатания на клавиатуре) и высокую надежность аутентификации, к недостаткам — сложность реализации и дороговизну, а также необходимость в дополнительном оборудовании и больших вычислительных ресурсах.

Аутентификация по уникальным параметрам использует сравнение каких-либо параметров человеческого тела (отпечатков пальцев, ладони, речи, сетчатки глаза, характеристик почерка) с их цифровыми образами, записанными в память системы, и является самым надежным методом проверки. Преимущество этого метода состоит в высокой надежности аутентификации пользователя, недостатки — высокая цена и необходимость наличия дополнительного оборудования.

5. ***Криптографические методы защиты данных*** — это методы защиты данных с помощью криптографического преобразования, под которым понимается преобразование данных шифрованием или выработкой имитовставки.

Шифрованием называется некоторое обратимое однозначное преобразование данных, делающее их непонятными для неавторизованных лиц.

Специалисты считают, что шифрование является одним из самых надежных средств обеспечения безопасности данных.

Метод защиты информации шифрованием подразумевает обязательное выполнение следующих требований. Никто, кроме хозяина данных, и лиц, которым разрешен доступ к этим данным, не должен знать самого алгоритма преобразования данных и управляющих данных для такого алгоритма (ключей).

Основными криптографическими методами защиты информации являются следующие:

• шифрование с помощью датчика псевдослучайных чисел;

• шифрование с помощью криптографических стандартов шифрования данных (с симметричной схемой шифрования), использующих проверенные и апробированные алгоритмы шифрования данных, например, американский стандарт шифрования данных DES;

• шифрование с помощью систем с открытым ключом (с асимметричной схемой шифрования), в которых для шифрования данных используется один ключ, а для расшифровки — другой.

Первый ключ не является секретным и может быть опубликован для использования всеми пользователями системы.

Второй ключ является секретным и используется получателем зашифрованной информации для ее расшифровки. Примером может служить метод криптографической защиты информации с известным ключом RSA.

Средства криптографии, реализованные в аппаратных, программных и программно-аппаратных комплексах защиты информации, включают:

• средства обеспечения конфиденциальности данных (шифрование для защиты как от несанкционированного доступа со стороны злоумышленника, так и от компьютерных вирусов);

• средства обеспечения подлинности документов и сообщений (электронная цифровая подпись);

• средства обеспечения целостности данных с целью обнаружения случайных и преднамеренных искажений (код аутентификации сообщения, имитовставка, хеш-функция);

• средства защиты программ от несанкционированного копирования и распространения;

• средства управления ключевой системой (выполнение задач генерации, распределения, использования, управления сменой, хранения, уничтожения и восстановления ключей).

Криптографические средства защиты информации осуществляют закрытие (шифрование) информации при ее обработке, накопле-

нии и передаче по линиям связи. При этом система считается практически закрытой, если "взломщик" шифротекста (криптограммы) должен затратить так много времени и вычислительных ресурсов для ее решения (расшифровки), что результирующая стоимость его работы не оправдывает затрат на получение расшифрованного (исходного) сообщения.

Использование криптографической техники многие эксперты по компьютерной безопасности считают основным, если не последним бастионом защиты от вирусной инфекции, во всяком случае, применение шифрования может сильно затруднить распространение вирусов.

Это относится к любым вирусам, присутствие которых криптографические программы могут обнаружить по изменению контрольных сумм файлов и других характеристик. С другой стороны, эта защита срабатывает, как правило, после того, как заражение уже состоялось, и создает определенные неудобства пользователям, а также персоналу, ответственному за обеспечение безопасности.

Так как расшифровка возможна только в том случае, когда зашифрованные данные не были искажены, криптографическую защиту можно использовать для обеспечения целостности данных.

Если захватчик как-либо исказил (модифицировал) зашифрованные данные, то факт нарушения безопасности будет выявлен при первой же попытке расшифровки, поскольку в расшифрованных данных появятся искаженные участки.

При сравнении классического алгоритма DES и криптографического алгоритма с открытым ключом RSA можно отметить как преимущества алгоритма DES — теоретическую криптостойкость (у алгоритма RSA — практическая) и высокую скорость работы, так и преимущество алгоритма RSA — отсутствие необходимости в строго засекреченном обмене ключами.

При использовании алгоритма RSA только один пользователь должен считаться заслуживающим доверия, так как другие пользователи не способны выполнить операции, которые может выполнить этот определенный пользователь.

Для многих практических приложений имеет смысл применять гибридную криптографическую систему, в которой используются преимущества как алгоритма DES, так и алгоритма RSA. В таких системах криптографические системы с открытым ключом применялись бы только в процессах управления ключами для создания общих ключей с последующим их применением в классических криптографических системах.

Следует отметить, что при всей привлекательности и трудности преодоления защита с помощью шифрования обладает некоторыми негативными чертами, которые в нашей стране особенно существенны. Применение этого уровня защиты означает для персонала (имеется в виду персонал, ответственный за обеспечение секретности) новую жизнь, полную жестко регламентированных предопределенных действий.

Необходимо обеспечить ежедневную службу резервирования информации, поскольку ошибки в чтении отдельных секторов или кластеров защищенной шифрованием области могут приводить к потере информации из всей области.

Отсюда повышенные требования к качеству дисков, на которых расположена шифрованная область; абсолютные требования к качеству и регулярности службы резервирования информации; повышенный риск, по меньшей мере, дополнительные потери времени на восстановление информации в случае сбоев.

Эти факторы существенны при работе с любым программным обеспечением или аппаратурой, обеспечивающей криптографический уровень защиты данных.

Рекомендовать применение такой защиты можно только при наличии качественного, надежно работающего оборудования, организации надежной автоматической службы резервирования информации и наличии действительной потребности в столь сложной защите данных.

6. ***Организационные средства защиты данных*** — организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации автоматизированной информационной системы предприятия для обеспе-

чения защиты информации. Организационные мероприятия охватывают все структурные компоненты системы на всех этапах их жизненного цикла (строительство помещений, проектирование системы, монтаж и наладка оборудования, испытания и эксплуатация).

В процессе эксплуатации автоматизированной информационной системы одним из универсальных средств защиты является создание резервных копий системы целиком или ее наиболее важных компонентов. Имея в запасе резервную копию и столкнувшись с искажением поврежденных данных или их потерей, для продолжения нормальной работы достаточно просто извлечь копию утерянных данных.

Многими вычислительными центрами принято хранить три последние копии системы по схеме "дед — отец — сын". Копии должны храниться в надежном месте, исключающем возможность уничтожения. В то же время должна существовать возможность их оперативного использования. В некоторых случаях целесообразно хранение двух и более копий каждого набора данных.

Например, одна копия может храниться в сейфе, находящемся в границах доступа персонала системы, а другая — в другом здании. В случае сбоя оборудования в системе используется первая копия (оперативно), а в случае его уничтожения (например, при пожаре) — вторая.

Важным считается установление определенной дисциплины и порядка копирования. Нарушение этой дисциплины должно караться не менее серьезно, чем любое нарушение безопасности.

Конечно, создание и хранение резервных копий требует определенных затрат ресурсов системы. Но все затраты с лихвой окупаются за счет обеспечения безопасности системы; кроме того, в современных системах существует немало средств, специально предназначенных для создания резервных копий и существенно облегчающих выполнение копирования.

7. ***Законодательные средства защиты данных*** определяются законодательными актами страны, которыми регламентируются правила использования, обработки и передачи ин-

формации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

8. ***Морально-этические средства защиты данных*** реализуются в виде всевозможных норм, которые сложились традиционно или складываются по мере распространения вычислительной техники и средств связи в данной стране или обществе. Примером таких норм является Кодекс профессионального поведения членов Ассоциации пользователей ЭВМ США.

Системный подход к защите информации

В настоящее время существуют два основных подхода к проблеме обеспечения информационной безопасности — фрагментарный (редукционистский) и системный (комплексный).

Фрагментарный подход к защите информации ориентируется на противодействие строго определенным угрозам при определенных условиях. Примером реализации такого подхода может быть использование в защите специализированного антивирусного средства.

Отличительными чертами данного подхода являются:

- локальность действия;
- отсутствие единой защищенной среды обработки информации;
- потеря эффективности защиты при видоизменении угрозы.

Следовательно, фрагментарный подход к защите информации может применяться только в ограниченных пределах и лишь для обеспечения безопасности относительно простых информационных систем. Однако важнейшим свойством реальных отраслевых и территориальных автоматизированных информационных систем является их сложность и несводимость к механической "сумме" составляющих их частей.

Особенностью *системного подхода* к защите информации является создание защищенной среды обработки, хранения и передачи информации, объединяющей разнородные методы и средства противодействия угрозам: программно-технические, правовые, организационно-экономические. Организация подобной защищенной среды позволяет гарантировать определенный

уровень безопасности автоматизированной информационной системы.

Системный подход к защите информации базируется на следующих ***методологических принципах***:

- принципе конечной цели — абсолютного приоритета конечной (глобальной) цели;
- принципе единства — совместного рассмотрения системы как целого и как совокупности частей (элементов);
- принципе связности — рассмотрения любой части системы совместно с ее связями с окружением;
- принципе модульного построения — выделения модулей в системе и рассмотрения ее как совокупности модулей;
- принципе иерархии — введения иерархии частей (элементов) и их ранжирования;
- принципе функциональности — совместного рассмотрения структуры и функции с приоритетом функции над структурой;
- принципе развития — учета изменяемости системы, ее способности к развитию, расширению, замене частей, накапливанию информации;
- принципе децентрализации — сочетания в принимаемых решениях и управлении централизации и децентрализации;
- принципе неопределенности — учета неопределенностей и случайностей в системе.

Обеспечение информационной безопасности персональных компьютеров

Защита процессора и оперативной памяти персонального компьютера предусматривает:

- отслеживание попыток блокирования доступа к процессору;
- контроль за появлением в оперативной памяти резидентных программ;
- защиту системных данных;
- очистку остатков секретной информации в неиспользуемых областях оперативной памяти.

Существующие операционные системы персональных компьютеров (например, MS DOS, PC DOS) изначально были рассчитаны на работу в однопрограммном режиме и таких мер защиты не имели. Считалось, что пользователь ПК всегда может в сомнительных случаях осуществить перезагрузку операционной системы и устранить резидентные программы или выключить компьютер для прекращения работы программы.

Сейчас оперативную память контролируют некоторые антивирусные программы. Более сложные процедуры контроля доступа к оперативной памяти и процессору возможны только в многопрограммных операционных системах (например, DR DOS и среда Windows).

Защита встроенного накопителя на жестком магнитном диске составляет одну из главных задач защиты персонального компьютера от чужого вторжения.

Можно назвать несколько типов программных средств, способных решать задачи защиты:

- средства, обеспечивающие защиту от любого доступа к жесткому диску;
- защита диска *от записи (чтения)*;
- контроль за обращениями к диску;
- средства удаления остатков секретной информации.

Защита встроенного жесткого диска от доступа обычно осуществляется путем применения паролей для идентификации пользователя (парольная идентификация).

Пакет программ *Norton Utilities* содержит ряд утилит для обеспечения безопасности накопителей на магнитных дисках:

- утилита DiskMonitor предотвращает попытки записи на диск без санкции пользователя;
- утилита Diskreet зашифровывает и обеспечивает парольную защиту файлов, каталогов и логических дисков путем создания защищенного паролем виртуального диска, все файлы которого зашифрованы;

• утилита WipelInfo физически стирает информацию, содержащуюся в файлах, на целых дисках или удаленную логически, после чего она не может быть восстановлена никакими средствами.

Рассмотрим аппаратные и программно-аппаратные методы защиты персональных компьютеров.

Очень простым, но весьма эффективным средством обеспечения безопасности данных и защиты от вирусов является специальная конструкция компьютера, благодаря которой воровство данных или заражение файлов или файловых систем вирусами становится невозможным.

Так, фирма *Earth Computer* из Калифорнии делает серию компьютеров EarthStation, приспособленных для работы в локальной сети, но не имеющих шинных разъемов, т. е. принципиально не расширяемых. Главная (и единственная) плата этого компьютера расположена в клавиатуре.

Управление клавиатурой, видеоадаптер и сетевой адаптер объединены на этой плате. В компьютере находится специальный вариант BIOS, позволяющий загружать DOS по локальной сети.

Нельзя отказать разработчикам таких компьютеров в остроумии: если некуда положить ворованное, то лучше и не красть; относительно заражения вирусами проблема решается так же, как с воровством, — на компьютере нечего заражать.

Большинство фирм защищают свое оборудование с помощью одного из вариантов парольной защиты, более или менее интегрированной с оборудованием. Так, во многих персональных компьютерах предусмотрена возможность установки пользовательского пароля из программы настройки BIOS Setup.

К числу таких фирм относятся, например, *Compaq* и *Hewlett-Packard*. Правда, для них этот вид деятельности не является основным, и те варианты защиты, которые фирмы предоставляют клиентам, не слишком совершенны.

Compaq разработала для своих моделей DeskPro специальную версию BIOS, содержащую элементы защиты от несанкцио-

нированного использования компьютера. Так, при загрузке компьютера при включении питания еще во время процедуры POST требуется указать правильный пароль, чтобы машина продолжала работу.

Сам пароль хранится в области CMOS и при большом желании, безусловно, может быть стерт (фирма *Hewlett-Packard* предусматривает хранение в специальной области CMOS предыдущей конфигурации компьютера, и при нажатии кнопки эта конфигурация может быть восстановлена в обычной области CMOS), но для затруднения доступа к "внутренностям" компьютера фирма снабжает корпус качественным замком (физический уровень защиты).

Кроме этой возможности, в BIOS реализованы программы, поддерживающие следующие области разделения доступа: возможность быстрого запирания компьютера, защиту серверного состояния компьютера, защиту жесткого диска, гибкого диска, последовательного и параллельного портов. Запуск защитных программ из BIOS регулируется переключателями на плате компьютера (аппаратный уровень защиты).

Учитывая неусыпную заботу коммерсантов о конфиденциальности данных, компьютеры Vectra фирмы *Hewlett-Packard* снабжены "замком", который приводится в действие нажатием кнопки на корпусе. После этого проникнуть в машину можно лишь набрав пароль с клавиатуры. Такая блокировка клавиатуры может применяться при работе как с DOS, так и с UNIX.

Важным элементом данной серии компьютеров является двухуровневая парольная защита, встроенная в BIOS. Кроме того, в режиме сетевого сервера предусмотрена загрузка системы и при запертой клавиатуре, что предотвращает возможность несанкционированного проникновения в нее.

При использовании персонального компьютера в качестве станции сети можно запретить загрузку с системного гибкого или жесткого диска, при этом загрузка будет возможна только с сетевого сервера.

Последнее позволяет, в частности, не удалять из накопителя гибкий диск в момент загрузки. Предусмотрен также режим блокировки вывода на последовательный и параллельный порты и записи на гибкие диски для предотвращения утечки важной информации. Данные возможности позволяют отсечь большой процент нелегальных попыток забраться в компьютер.

Упомянутые выше аппаратные доработки плат, усовершенствования BIOS улучшают условия работы на персональном компьютере с точки зрения безопасности, приучают пользователя к порядку и одновременно ограничивают возможность случайного заражения, хотя проблему комплексной защиты от вирусов, конечно, не решают.

Серия компьютеров Netmate фирмы *Datamedia* оборудована специальным устройством Securecard reader — считывателем карт безопасности. Карты безопасности по исполнению являются вариантом кредитных карт; на них на магнитном носителе с помощью специальной аппаратуры, которая имеется только в распоряжении администратора, делается запись о пользователе: его имя, пароль и описываются все полномочия, которые он получает при входе в систему.

В частности, на карте записано, сколько раз пользователь может пытаться указать пароль при входе. Таким образом, случайная потеря карты безопасности или ее кража не позволяют злоумышленнику получить доступ к компьютеру: если имя пользователя еще можно узнать, не привлекая внимания, то пароль ему неизвестен. Только сознательная передача карты безопасности кому-то одновременно с разглашением пароля может открыть доступ к компьютеру постороннему лицу.

При объединении таких компьютеров в вычислительную систему администратор системы создает карту безопасности для легальных пользователей. На этой карте, помимо уже перечисленной информации, описывается профиль пользователя. Например, определяется, какие из локальных устройств (гибкие диски, жесткие диски, последовательные и параллельные порты) доступны этому пользователю, с каких локальных или сетевых устройств он может загружаться.

Предусмотрена и трансляция паролей: тот пароль, который назначается пользователю, как правило, легко запоминающийся, но вовсе не тот, с которым работает система.

В программное обеспечение встроены специальные возможности, которые повышают уровень "тревожности" в случае возникновения ненормальных ситуаций. При попытке просто выдернуть карту безопасности из считывателя доступ к компьютеру намертво блокируется, пока в считыватель не будет вставлена та же карта безопасности. И если такая ошибка для легального пользователя несущественна, для злоумышленника такой оборот дела совершенно неприемлем.

При неправильном указании пароля (если превышено количество попыток, разрешенное для данного пользователя) машина также блокируется, и только администратор сможет "оживить" ее. Таким образом, все случаи нарушения режима секретности немедленно становятся достоянием администрации.

Перечисленные особенности данной системы — организация определенным образом работы пользователя, запрещение отдельных опасных действий типа запуска программ или загрузки с носителей, ограничения на использование определенных ресурсов системы типа сетевых карт, последовательных портов, повышенный уровень тревоги — резко уменьшают размеры ущерба от проникновения компьютерных вирусов.

Фирма *Software Security, Inc* (США) решает проблемы защиты программ, данных и компьютеров путем использования программно-аппаратных комплексов на базе электронных ключей собственного производства.

Выпускаемые фирмой электронные ключи присоединяются к параллельному порту Centronics компьютера. К выходному разъему ключа может быть присоединен принтер, другие электронные ключи SSI или ключи других производителей. Для команд, посылаемых принтеру, ключ абсолютно прозрачен. В рамках одной программы можно организовать одновременную работу как с принтером, так и с ключом.

При выполнении защищенной программы принтер нормально работает и в фоновом режиме. Всего к параллельному порту

может быть подключено до пятнадцати последовательно соединенных ключей SSI, и каждый из них будет работать независимо от других. Это означает, что на компьютере одновременно можно работать с пятнадцатью программами и все они будут защищены различными ключами. Таким образом, все изделия компании полностью отвечают требованию электрической совместимости.

"Сердцем" ключей SSI является патентованная заказная микросхема, содержащая постоянную, однократно программируемую и перепрограммируемую энергонезависимую память и реализующая сложную логическую функцию. Наличие такой микросхемы затрудняет эмуляцию электронного ключа и позволяет достичь высокой надежности защиты.

Защита программы с помощью ключа SSI выражается в том, что в защищаемую программу встраиваются фрагменты кода для обмена с электронным ключом и управления им. При исполнении защищенная программа подает на электронный ключ определенные команды, прямо или косвенно подтверждающие присутствие нужного ключа на порту. В зависимости от ответов электронного ключа программа реализует предусмотренную алгоритмом стратегию защиты.

Следующим шагом компании *Software Security, Inc* стала разработка нового семейства электронных ключей UniKey. Семейство UniKey включает ключи для DOS, Windows, UNIX, локальных сетей, устройства для параллельного и последовательного портов, микропроцессорные ключи, ключи с таймерами, счетчиками и др. Данное семейство ключей предоставляет широкий диапазон возможностей разработчику защиты.

С точки зрения разработчика защиты каждый ключ UniKey является совокупностью ресурсов: памяти, счетчиков числа пользователей, счетчиков запусков и др. Для удобства использования все ресурсы ключа сведены в специальную структуру — "запись приложения", причем в каждом ключе может содержаться несколько записей. В процессе защиты программы разработчик обращается к определенной "записи приложения", используя (явно или косвенно) ее поля.

В основе всех ключей этого семейства лежит общая логическая модель, они имеют следующие общие свойства:

1. *Уникальность.* Основополагающее свойство всех ключей UniKey, которое и дало название всему семейству. Каждый UniKey имеет уникальный идентификатор, устанавливаемый при его изготовлении. Процедуры обмена с ключом и обращения к памяти перестраиваются в зависимости от значения идентификатора, что позволяет говорить об уникальности защиты, созданной на базе UniKey. Под уникальностью защиты здесь понимается уникальность протокола взаимодействия с ключом. Важно отметить, что данное свойство протокола обеспечивается вне зависимости от того, какие программные средства использовались при создании защищенной программы.

2. *Универсальность.* Пакет программного обеспечения, поставляемый с каждым UniKey, включает целый набор средств для создания защиты:

- комплекс Aegis для автоматической защиты программ;
- библиотеку защищенных объектных модулей;
- комплекс ToolBox.

Наличие универсальности в обеспечении программными средствами удобно для разработчиков: каждый из них сам выбирает стратегию защиты, наиболее подходящую для его прикладных программ. Более того, существует возможность комбинировать предлагаемые средства: например, защитить с помощью Aegis программу, использующую "внутри" вызовы библиотеки ToolBox. Тем самым общий уровень защиты увеличивается.

3. *Унифицированность. Software Security* предлагает одинаковый набор программных средств для всех ключей семейства — объектные модули, ToolBox и Aegis. Естественно, "внутренняя начинка" программ и библиотек различна, но заказчики имеют практически один и тот же интерфейс при использовании различных типов UniKey. По существу, разработчик всегда обращается не непосредственно к ключу, а к "записи приложения", независимо от того, в каком ключе находится эта запись.

Это существенно упрощает переход с одного типа UniKey на другой. Например, если у пользователя, работающего с локальными ключами UniKey и библиотекой ToolBox, появилась необходимость использовать сетевую защиту, то ему достаточно заменить версию ToolBox на сетевую, не меняя схему защиты и не переделывая существенным образом код защищаемой программы.

Следует отметить, что существующие различия в интерфейсах обусловлены функциональными отличиями ключей: например, ключ с таймером предполагает процедуры работы со временем, тогда как для всех остальных устройств они не нужны.

4. *Модифицируемость*. Особенностью семейства UniKey является то, что ресурсы всех ключей можно модифицировать: обновлять счетчики запусков и число пользователей, изменять конфигурацию памяти и т. д. В процессе защиты программы разработчик заносит в ключ определенные ресурсы путем установки полей "записи приложения".

После того как ключ UniKey попал к конечному пользователю программы, разработчик имеет возможность модифицировать ресурсы ключа (т. е. устанавливать переменные поля "записи приложения") дистанционно с помощью специальной системы RTS.

Данное свойство позволяет строить гибкие и удобные для пользователей стратегии продаж, включающие преобразование по телефону демо-версий в рабочие программы, обновление исчерпанных ресурсов, дистанционное изменение эксплуатационных характеристик работающего комплекса.

5. *Секретность*. Все ключи семейства, за исключением UniKey для параллельного порта, содержат внутри специализированный микропроцессор. Это конструктивное решение позволило обеспечить стабильную работу с ключом на персональных компьютерах под управлением многозадачных операционных систем (Windows NT, Windows 95, OS / 2, UNIX) и, самое главное, существенно повысить секретность обмена за счет использования сложного шифрованного протокола. Достаточно сказать, что в микро-

программах для UniKey аппаратно заложены элементы шифровального двухключевого алгоритма RSA.

Защита от компьютерных вирусов. По мере распространения и совершенствования компьютерных вирусов проблема сохранности данных в вычислительных системах приобретает все большую остроту. По всей видимости, нет оснований ожидать ее кардинального решения какими-либо техническими или программными средствами в ближайшем будущем. Достаточно надежно решить ее могла бы специально спроектированная операционная система, не позволяющая создавать программы типа вирусов.

Операционная система MS DOS, отличающаяся практически полным отсутствием защиты от несанкционированных действий, облегчает разработку компьютерных вирусов. Однако важно понимать, что компьютерные вирусы не являются программами, использующими ошибки или недостатки конкретной операционной системы.

Для обеспечения своего функционирования вирусу достаточно лишь нескольких вполне обычных операций, используемых большинством "нормальных" программ. Поэтому принципиально невозможно существование универсального метода, защищающего операционную систему MS DOS от распространения любого вируса.

Внедрение вируса в компьютерную систему можно обнаруживать на разных этапах: до внедрения, в момент заражения системы, после внедрения и в момент нанесения системе повреждений. Каждый из этих методов имеет свои сильные и слабые стороны. Наряду с естественными вирусами, для борьбы с компьютерными вирусами может применяться целый комплекс мер: технических, организационных, юридических.

Среди важнейших мер по защите от вирусов отметим следующие:

- резервирование;
- профилактику;
- ревизию;
- фильтрацию;

• вакцинацию;

• терапию.

Резервирование включает ежедневное ведение архивов измененных файлов и регулярное получение копий системных областей накопителей с помощью программ Rescue, Image, IniTrakd, DiskEdit из пакета Norton Utilities. Это самый важный, основной метод защиты от вирусов. Если в конце дня скопировать на дискету результаты проделанной работы, ущерб от любого компьютерного вируса будет минимальным. Остальные методы не могут заменить ежедневное архивирование, хотя и повышают общий уровень защиты.

К методам *профилактического характера* относятся:

• раздельное хранение вновь полученных и эксплуатирующихся программ;

• разбиение жесткого диска с помощью программы Disk Manager на "непотопляемые отсеки" — зоны с установленным атрибутом "только чтение";

• хранение неиспользуемых программ в архивах;

• использование специальной "инкубационной" зоны для записи новых программ с дискет и др.

Ревизия — это обнаружение компьютерного вируса до или после его внедрения в вычислительную систему.

Несомненно, наиболее привлекательно было бы обнаружить вирус до того, как он активируется и начнет выполнять какие-либо действия. К сожалению, обнаружить таким способом можно лишь те вирусы, которые были известны ко времени написания этой программы.

По всей видимости, не существует метода, позволяющего автоматически отличать программу с вирусом от "чистой", если либо вирус, либо "чистая" программа не были известны заранее. Поэтому такие программы обречены на быстрое моральное старение по мере появления новых вирусов.

Тем не менее этот метод дает возможность фактически не допустить известные вирусы в компьютер, если проверять дискеты перед первым их употреблением. Сканирование диска программами-детекторами требует немного времени и должно

производиться периодически, когда для этого есть свободное время, а также при поступлении нового программного обеспечения.

Необходимо обращать особое внимание на чистоту модулей, сжатых утилитами типа PKLITE, DIET или LZEXE, файлов в архивах (ZIP, ARJ, LZH, ARC и т. д.) и данных в самораспаковывающихся файлах, созданных архиваторами или утилитами.

Если случайно упаковать файл, зараженный вирусом, то обнаружение и удаление такого вируса без распаковки файла практически невозможно. В данном случае типичной будет ситуация, при которой все антивирусные программы сообщат о том, что от вирусов очищены все диски, но через некоторое время вирус появится вновь.

Из большого разнообразия программ-антивирусов можно рекомендовать Scan (*McAfee Associates*), Microsoft AntiVirus и Aidstest (АО "Диалог Наука", Д. Н. Лозинский). Две последние могут также исправлять зараженные программы и стирать испорченные. Например, программа Aidstest обнаруживает и обезвреживает все известные типы вирусов на *логических дисках и в памяти машины.*

Кроме того, Aidstest довольно надежно контролирует собственное здоровье относительно большинства типов вирусов. При обнаружении собственного заражения новым типом вируса Aidstest выдает соответствующее сообщение и прекращает работу. В связи с постоянным появлением новых вирусов и их модификаций обновление программы Aidstest производится несколько раз в месяц, и зарегистрированный пользователь всегда будет иметь самую последнюю версию.

Одним из наиболее популярных является пакет Norton AntiVirus, обеспечивающий быстрое сканирование и широкий спектр средств (профилактику, обнаружение, восстановление) для DOS и Windows 3.1.

Метод обнаружения вируса после его внедрения в систему представляет большие возможности для обнаружения ранее неизвестных вирусов. В основе его лежит контроль сохранности инфор-

мации в тех частях системы, куда могут внедриться вирусы. Основные данные о диске сохраняются в таблице (образы системного загрузчика винчестера и загрузочных секторов, список номеров сбойных кластеров, схема дерева каталогов и информация о всех контролируемых файлах).

Кроме этого, таблица может содержать доступный DOS объем оперативной памяти (заражение большинством загрузочных вирусов приводит к ее изменению), количество установленных винчестеров, таблицы параметров винчестера в области переменных BIOS (Hard Disk Parameter Table) и другую информацию.

Во время последующих запусков программ-ревизоров полученные данные сравниваются с эталоном. Внедрение любого, даже неизвестного, вируса будет обнаружено по несовпадению контрольных значений.

Однако такое несовпадение не всегда является следствием деятельности вируса. В частности, во многих программных пакетах (Turbo C, Turbo Pascal) программы-конфигураторы вносят настроечные изменения прямо в код программы. После этого программа вирусного контроля может выдать ошибочное предупреждение о заражении вирусом. Требуется некоторая сноровка, чтобы научиться правильно определять причины таких предупреждений, а не стирать в панике все файлы.

Другим уязвимым местом такой системы обнаружения вируса является установка новых программ на компьютер. Система вынуждена считать, что все впервые перенесенные на компьютер программы — "чистые", т. е. не содержат вируса, поскольку для них еще не известны эталонные контрольные значения. Это очень сильно затрудняет поиск источника заражения компьютера. Если файл уже содержит вирус, он не будет изменяться в дальнейшем, значит, и не будет отмечен системой.

Еще один недостаток данной системы — сложность восстановления после вторжения вируса. В простейшем случае такие системы выдают только список файлов, у которых контрольные значения не совпадают с эталоном. Единственный способ восстановле-

ния — замена этих файлов на "чистые" с архивного носителя информации.

Самой лучшей среди программ, реализующих этот метод, считается антивирусная программа-ревизор диска Advanced Diskinfoscope (ADinf) Д. Ю. Мостового. От всех существующих в настоящее время антивирусных программ ADinf отличается тем, что она работает с диском непосредственно по секторам через BIOS, не используя DOS, что позволяет успешно обнаруживать казавшиеся невидимыми так называемые "стелс"-вирусы, берущие на себя более 20 функций DOS, а также вирусы в дисковом драйвере, в том числе новые вирусы, неизвестные ранее.

Терапия — деактивация конкретного вируса в зараженных программах с помощью специальной программы-антибиотика или восстановление первоначального состояния программ путем "пожирания" всех экземпляров вируса в каждом из зараженных файлов или дисков с помощью программы-фага.

Абсолютное большинство существующих фагов использует знание конкретного вируса, что делает их независимыми от программы, которую они лечат, но привязывает к излечиваемому ими вирусу.

Как видно из приведенного выше материала, имеются несколько типов программных средств защиты от вирусов. Если попытаться наметить иерархию программных средств защиты по их вкладу в безопасность, то представляется, что на первом месте находятся программы-архиваторы.

Следующими по важности являются программы-ревизоры, позволяющие с помощью подсчета контрольных сумм определять целостность программ и данных. Они должны входить в арсенал каждого пользователя и регулярно использоваться в начале и конце каждого сеанса работы с ПК.

На третьем месте по важности находятся резидентные программы-фильтры, хотя степень обеспечиваемой ими защиты не стоит переоценивать, и программы-вакцины. И наконец, скромное четвертое место занимают программы-фаги, обеспечивающие возможность восстановления исходного состояния программы, зараженной конкретным вирусом.

Кроме чисто программных средств защиты от вирусов, существуют еще и программно-аппаратные. Преимуществом таких антивирусных средств является то, что они, в отличие от программ-антивирусов, начинают работать еще до загрузки операционной системы и, следовательно, способны отслеживать и обезвреживать в момент активизации даже загрузочные вирусы.

Действие программно-аппаратных комплексов заключается в том, что они постоянно следят за проявлениями любой специфической активности, характерной для компьютерных вирусов.

Поскольку они ориентированы на распознавание не самих вирусов, а производимых ими действий, для таких комплексов не имеет значения тип вируса, они не нуждаются в модификации при обнаружении каждого нового вируса и не требуют дополнительного времени на сканирование дисков. К ним относятся антивирусный комплекс Sheriff, антивирусная плата Thunderbyte.

Аппаратно-программный комплекс Sheriff обеспечивает практически 100-процентную защиту компьютеров типа IBM PC / AT от любых видов вредоносных воздействий:

- компьютерных вирусов;
- "троянских программ";
- ошибочных или злоумышленных действий пользователей;
- ошибок в отлаживаемом программном обеспечении.

Утверждение о надежности защиты основано на применении специального аппаратного контроллера, который фиксирует все "незаконные" операции записи на винчестер.

Особенно эффективно применение комплекса Sheriff на компьютерах, работающих в сети.

Аппаратно-программный комплекс Sheriff состоит из аппаратного блок-контроллера, вставляемого в свободное гнездо на материнской плате компьютера, и программного обеспечения, поставляемого на инсталляционном носителе.

Sheriff надежно защищает операционную систему и контролируемые файлы от уничтожения, изменения или удаления,

пользователь даже при желании не сумеет выполнить данные действия. Доступ к винчестеру компьютера осуществляется по паролю, запрашиваемому при начальной загрузке с винчестера. Если загрузку произвести, к примеру, с флешки, то винчестер для ОС становится недоступным.

Аппаратные средства защиты от компьютерных вирусов, основанные на принципе перлюстрации команд к физическому устройству, реализуют грубую, но действенную, системно независимую защиту. К ним относятся Disk Defender (*Director Technologies, Inc*), Guard Card (*North Bank Corporation*), Immunetec PC (*Zeus*) и Trispan (*Micronics*).

Блокировка распространения любых типов вирусов осуществляется только в защищенных областях диска. Правда, заодно в этих областях становятся невозможными любые модификации данных: правка текстовых файлов редактором, трансляция программ и т. д. Еще один недостаток этой защиты состоит в том, что защищаемой областью является физическое место на диске, и какие каталоги, файлы, какая часть файловой структуры окажутся в этой физической области, определяется в результате кропотливой настройки файловой системы.

С другой стороны, защита в определенных ситуациях оказывается обременительной настолько, что, очевидно, ее необходимо отключать совершенно для каких-то областей диска или всего диска в целом (при установке нового программного обеспечения, обновлении и т. п.).

Так как во время отключения защиты все становится уязвимым, как на обычном компьютере, при выполнении таких операций следует проявлять повышенное внимание и аккуратность. Впрочем, даже если произойдет заражение, после включения защиты распространение вируса на защищенной части будет невозможно, что, вероятно, минимизирует возможный ущерб.

Во многих современных персональных компьютерах предусмотрена возможность включения антивирусной защиты из программы настройки BIOS Setup. Такая защита будет отслеживать, например, попытки изменить загрузочный сектор винчестера. Для расширения

возможностей защиты компьютера необходимо приобрести и установить в компьютер пакет антивирусных средств, загружающихся в качестве расширения BIOS.

Компьютерная гигиена — это совокупность организационных и профилактических мероприятий по защите компьютерной системы от вирусов. Она предусматривает выполнение ряда рекомендаций при использовании вычислительных систем, в особенности персональных компьютеров. Строгое выполнение этих правил позволит свести риск "заболевания" компьютера к минимуму (но не исключить вообще), однако может оказаться обременительным и дорогим. В каждом случае нужно выбирать разумный компромисс.

Приведем рекомендации компьютерной гигиены:

1. Использовать только легально полученное программное обеспечение (поставляемое на "фирменных" носителях информации), разработчик которого известен и имеет хорошую репутацию. Не следует переписывать программное обеспечение с других компьютеров, так как оно может быть заражено вирусом. Кроме того, вирусы могут использоваться для защиты программного обеспечения от незаконного копирования.

2. Приобретаемые программы должны внимательно анализироваться системным программистом перед их установкой.

3. Сразу же после получения нового программного обеспечения должна быть изготовлена его рабочая копия (на машине, известной как "чистая"). Оригинал должен быть защищен от записи и храниться отдельно.

4. Все принесенные извне носители перед использованием следует проверить на наличие вируса с помощью программ-детекторов. Это полезно делать даже в тех случаях, когда вы собираетесь использовать на этих информационных носителях только файлы с данными, — чем раньше вы обнаружите вирус, тем лучше.

5. Если вы хотите работать с какой-то новой для себя программой, в которой может оказаться вирус, то перед работой с ней следует позаботиться, чтобы на компьютере была запущена резидентная программа — фильтр для защиты от вируса. Лучше всего новое программное обеспечение испытывать на отдельном компьютере, не содержащем важной информации.

6. Необходимо периодически делать резервные копии (архивировать) те файлы, которые вы создали или изменяли. Это позволит уменьшить потери в случае поражения компьютера вирусом. Перед архивацией файлов целесообразно запустить программы-детекторы, чтобы убедиться в отсутствии вируса в компьютере и избежать помещения испорченных или зараженных файлов в архив. В противном случае ваш архив превратится в постоянного поставщика вируса при обновлении копий на вашем компьютере.

7. Следует защищать от записи флешки с файлами, которые не надо изменять. На жестком диске целесообразно создать логический диск, защищенный от записи, и поместить на него программы и данные, которые надо только использовать, но не изменять.

8. Если нет необходимости загружать операционную систему с носителя, измените в программе настройки BIOS последовательность загрузки (System Boot Up Sequence, раздел Advanced Setup) на C. После этого загрузка будет осуществляться сразу с винчестера.

9. Если вы хотите перезагрузить компьютер с флешки или другого носителя, то пользуйтесь только защищенным от записи "эталонным" носителем с операционной системой. Полезно создать и хранить в доступном месте "системную" флешку, т. е. флешку, с которой можно загрузить операционную систему MS DOS. На ней не должны находиться все программы, входящие в состав MS DOS, но должны присутствовать программы Format, Label, Msav, Scandisk, Sys, Undelete, Vsafe, а также программы DiskEdit, DiskTest и DiskTool из пакета Norton Utilities, программы-антивирусы Aidstest и Scan. Если вы привыкли работать с программами-оболочками типа Norton Commander, то их также следует скопировать на используемый в данном случае носитель (желательно более ранних версий: они занимают меньше места).

10. Желательно вставить в командный файл Autoexec.bat, выполняемый при начальной загрузке MS DOS, вызов программы-ревизора ADinf для проверки изменений в файлах.

11. Регулярно, например раз в неделю, проводите профилактику винчестера своего компьютера с помощью следующих утилит:

• программы проверки дисков ScanDisk;

• программы оптимизации дисков Defrag (или SpeedDisk из Norton Utilities);

• программ резервирования системной информации Rescue, Image и IniTrakd из пакета Norton Utilities.

ScanDisk сообщит о всех неполадках в файловой системе (потерянных файлах, перекрестных ссылках), если таковые имеются. Они могут возникнуть как в результате действий вируса (например, при поражении вирусом "Driver-1024 / Dir" — большое количество перекрестных ссылок), так и при системных сбоях. Рекомендуется запускать ScanDisk также после каждой перезагрузки, связанной с "зависанием" компьютерной системы. Что-либо исправлять программой ScanDisk можно только убедившись в отсутствии вирусов в системе.

Применение программ оптимизации связано с тем, что наиболее распространенным разрушительным действием вируса является уничтожение информации, а существующие методы восстановления файлов с помощью команды Undelete (или программы Unerase из Norton Utilities) способны правильно восстанавливать лишь те файлы, которые записаны на диск подряд, в виде цепочки последовательных кластеров.

Поэтому для успешного восстановления файла необходимо, чтобы флешка или винчестер периодически обрабатывались программами дефрагментации дисков, которые реорганизуют записи на диске таким образом, чтобы все они располагались подряд. После запуска программа оптимизации оценит степень фрагментации обрабатываемого диска и выдаст свою рекомендацию: оптимизировать его или нет.

С помощью программы Rescue создается "спасательный" носитель, хранящий жизненно важную информацию о настройке вашего компьютера. Эта же программа восстанавливает потерянные данные CMOS, системный загрузчик винчестера, загрузочный сектор, модули MS DOS и т. д.

Программа Image делает "моментальный снимок" жизненно важных областей диска и сохраняет его в файле Image.dat. При искажении или разрушении системных блоков винчестера возможно

их восстановление программой Unformat с использованием данных своевременно созданного и сохраненного на носителе файла Image.dat.

Программа IniTrakd сохраняет системные и инициализационные файлы DOS и Windows и восстанавливает сохраненную информацию.

12. Следует ограничивать доступ посторонних к вычислительной системе, особенно если они имеют свои флешки. Очень часто причиной заражения компьютера вирусом являлась принесенная игра. В том случае, если избежать доступа случайных лиц к компьютеру невозможно (например, в учебном центре), целесообразно все или почти все программы, находящиеся на жестком диске компьютера, располагать на логическом диске, защищенном от записи.

13. Обнаружив симптомы заболевания, предупредите об этом всех пользователей, работающих на этом компьютере. Сообщите об этом специалисту, занимающемуся вирусами, или системному программисту.

Поскольку ни один из методов сам по себе не обеспечивает надежной защиты от вирусов и достаточно быстрого устранения последствий вторжения вируса, необходимо применять комбинированные методы.

В случае заражения компьютерной системы вирусом единого рецепта действий нет, но самым лучшим будет приглашение грамотного и компетентного специалиста. Если сделать это по каким-либо причинам не удалось, как крайнюю меру можно предложить уничтожение всех программ и данных даже при подозрении на вирус и восстановление программного обеспечения с эталонов и копий.

Возможна и менее радикальная последовательность действий для предотвращения распространения вируса:

1. Выключить систему (отключить от источников питания). Это, во-первых, предотвратит дальнейшее размножение вируса, а во-вторых, позволит избавиться от резидентных вирусов в оперативной памяти.

2. Отключить все внешние линии связи (если они есть) для локализации вируса.

3. Установить защиту от записи на все возможные носители данных.

4. Включить систему, используя для загрузки эталонную версию MS DOS, поставляемую производителем, с носителя, защищенного от записи. При использовании самостоятельно изготовленной копии не исключено, что в ней тоже может содержаться вирус в результате небрежности при копировании.

5. Осуществить копирование всех программ и данных с носителя, где обнаружен вирус, на новый. Эти копии могут быть полезны как при анализе возникшей ситуации, так и в случае, если резервные копии были испорчены или утрачены. Необходимо пометить (лучше всего опечатать в отдельном конверте) носители с полученными копиями для предотвращения случайного использования и возможного распространения вируса.

6. Переформатировать все старые носители данных, на которых был обнаружен вирус. Это позволит уничтожить все вирусы, инфицирующие накопители (например, вирусы загрузчика).

7. Восстановить программное обеспечение из эталонных копий программ, хранимых на носителях, защищенных от записи.

8. Проверить целостность данных, в том числе и последних их копий, которые могли быть изменены вирусом. Для восстановления системы используются данные и их копии, прошедшие проверку. Чем раньше была сделана копия, тем меньше вероятность изменения ее вирусом.

9. Провести анализ зараженного программного обеспечения с привлечением компетентных специалистов. Результаты анализа могут быть использованы для борьбы с вирусом и предупреждения других пользователей. Первым шагом такого анализа должно стать использование средств обнаружения вирусов и выделение кодов вируса для дальнейшего исследования.

10. Запустить доступные пользователю программы диагностики и защиты в компьютерной системе, тщательно проверить работоспособность системы и при обнаружении отклонений в ее работе проконсультироваться со специалистами.

Защита информации в компьютерных сетях

Защита сети как единой системы складывается из мер защиты каждого отдельного узла и функций защиты протоколов данной сети.

Каждый узел сети должен иметь индивидуальную защиту в зависимости от выполняемых функций и возможностей сети.

Необходимо осуществлять на каждом отдельном узле:

- контроль доступа ко всем файлам и другим наборам данных, доступных из локальной сети и других сетей;
- контроль процессов, инициированных с удаленных узлов;
- контроль сетевого трафика;
- эффективную идентификацию и аутентификацию пользователей, получающих доступ к данному узлу из сети;
- контроль доступа к ресурсам локального узла, доступным для использования пользователям сети;
- контроль за распространением информации в пределах локальной сети и связанных с нею других сетей.

Обеспечение конфиденциальности обрабатываемой и передаваемой в сети информации, целостности и доступности ресурсов (компонентов) сети достигается с помощью специальных **механизмов защиты**: шифрования, цифровой подписи, контроля доступа, обеспечения целостности данных, аутентификации, заполнения текста, управления маршрутом и освидетельствования.

Механизм шифрования обеспечивает конфиденциальность передаваемых данных, а также информации о потоках данных. Существуют два способа шифрования: канальное (реализуется с помощью протокола канального уровня) и оконечное (реализуется с помощью протокола прикладного уровня).

В случае *канального шифрования* защищается вся передаваемая по каналу связи информация, в том числе и служебная.

Особенности данного способа:

- вскрытие ключа шифрования для одного канала не приводит к компрометации информации в других каналах;
- пользователь не принимает участия в выполняемых операциях;

• вся передаваемая информация, включая служебные сообщения, надежно защищена;

• вся информация оказывается открытой на промежуточных узлах — ретрансляторах, шлюзах и т. д.;

• для каждой пары узлов требуется свой ключ;

• алгоритм шифрования должен быть достаточно стоек и обеспечивать скорость шифрования на уровне пропускной способности канала, что приводит к необходимости реализации алгоритма шифрования аппаратными средствами.

Оконечное (абонентское) шифрование позволяет обеспечивать конфиденциальность данных, передаваемых между двумя прикладными объектами. При этом отправитель зашифровывает данные, а получатель их расшифровывает.

Особенности этого способа заключаются в следующем:

• защищенным оказывается только содержание сообщения, вся служебная информация остается открытой;

• при достаточно стойком алгоритме шифрования никто, кроме отправителя и получателя, восстановить информацию не может;

• маршрут передачи несущественен — в любом канале информация остается защищенной;

• для каждой пары пользователей требуется уникальный ключ;

• пользователь должен знать процедуры шифрования и распределения ключей.

В конкретном случае выбор способа шифрования зависит от результатов анализа риска и определения того, что более уязвимо — непосредственно отдельный канал связи или содержание сообщения, передаваемого по различным каналам.

Канальное шифрование быстрее, прозрачно для пользователя, требует меньше ключей. Оконечное шифрование более гибкое, может использоваться выборочно, однако требует участия пользователя.

Механизм цифровой подписи включает процедуры закрытия блоков данных и проверки закрытого блока данных. С помощью секретной ключевой информации отправитель фор-

мирует служебный блок данных, получатель на основе общедоступной информации (не позволяющей восстановить секретные данные) проверяет принятый блок и определяет подлинность отправителя. Сформировать подлинный блок может только пользователь, имеющий соответствующий ключ.

Механизм контроля доступа осуществляет проверку полномочий сетевого объекта на доступ к ресурсам.

Механизм сохранения целостности передаваемых данных обеспечивает целостность отдельного поля, блока и потока данных в целом. Целостность блока данных достигается благодаря добавлению к нему признака, значение которого является функцией от самих данных.

Защита целостности потоков данных (от переупорядочивания, добавления, повторов или удаления сообщений) осуществляется с использованием дополнительной формы нумерации (контроль номеров сообщений в потоке), меток времени и т. д.

Механизм аутентификации объектов сети использует пароли, методы проверки характеристик объекта, криптографические методы. Используемые методы могут совмещаться с процедурой троекратного обмена сообщениями между отправителем и получателем с параметрами аутентификации и подтверждениями.

Механизм заполнения текста используется для обеспечения защиты от анализа трафика. В качестве такого механизма может использоваться генерация фиктивных сообщений. В этом случае трафик имеет постоянную интенсивность во времени.

Механизм управления маршрутом позволяет использовать физически безопасные подсети, ретрансляторы, каналы. Оконечные системы при установлении попыток навязывания могут потребовать установления соединения по другому маршруту. Также может использоваться выборочная маршрутизация, когда часть маршрута задается отправителем в обход опасных участков.

Механизм освидетельствования используется для подтверждения характеристик данных, передаваемых между двумя и более объектами (целостность, источник, время, получатель). Подтверж-

дение обеспечивается третьей стороной (арбитром), которой доверяют все заинтересованные стороны и которая обладает необходимой информацией.

Реализация механизма управления доступом в компьютерных сетях

Одна из центральных проблем в обеспечении безопасности компьютерных систем — проблема несанкционированного (неавторизованного) доступа и способы его предотвращения.

Задача заключается в обеспечении такого порядка работы, при котором систему мог бы использовать только тот, кому ее разрешено использовать; чтобы каждый законный пользователь работал только со "своими" данными и не мог исказить, прочитать или удалить из системы данные, принадлежащие другому пользователю (если на то нет согласия хозяина); чтобы каждый законный пользователь мог выполнять только те операции, которые ему разрешено выполнять администратором системы.

Для начала каждому новому пользователю необходимо предоставлять только самый необходимый набор средств, без которых он вообще работать не сможет. По незнанию, неопытности или неосторожности такой пользователь может сотворить самые невероятные вещи: от простого удаления собственных данных до приведения в неработоспособное состояние всей системы в целом либо отдельных ее компонентов.

Вход в компьютерную систему состоит из процедур идентификации, аутентификации и авторизации.

Идентификация пользователя заключается в том, что он при выполнении каких-либо действий должен себя назвать, вернее, указать идентификатор, присвоенный данному пользователю в данной системе. Получив идентификатор, система сравнивает его значение с эталоном и в случае совпадения обеспечивает пользователю возможность работать с компонентами системы.

Для идентификации могут применяться специальные устройства, способные идентифицировать пользователя по некоторым его физическим характеристикам, например по отпечаткам пальцев,

спектральному составу голоса или даже по сетчатке глаза; различного рода магнитные карточки, специальные ключи и т. д.

После идентификации система обязательно проводит аутентификацию полученного идентификатора: проверяется содержательность указанного идентификатора для данной системы. Для проведения аутентификации пользователь должен выполнить некоторые явные действия (ввод пароля, ответы на тестовые вопросы). Механизмы, используемые для выполнения аутентификации, должны быть устойчивы к подлогу, подбору или подделке.

Максимальный уровень безопасности против всякого "подглядывания" обеспечивается запрещением неавторизованного доступа к компьютеру. Однако в системах, обеспечивающих доступ к компьютеру удаленному пользователю, проблема состоит в том, чтобы получить доказательства того, что пользователь именно тот, за кого он себя выдает (или кем себя называет). Такие доказательства — это или вариации на тему парольной защиты, или различные биометрические системы.

Для удаленных пользователей сейчас наиболее распространены системы обратного вызова. Эти устройства при первом доступе к ним внешнего пользователя не дают контакта с вызываемым компьютером, а требуют назвать пароль или еще каким-нибудь способом идентифицировать себя.

Если пароль назван правильно или идентификация пользователя прошла успешно, ему возвращается номер телефона, ассоциированный с этим пользователем. Устройство обратного вызова запрашивает указанный номер телефона для подключения и выполнения нормальной процедуры вхождения в систему.

Схемы раздачи паролей или обмен ключами легальных пользователей в развитых сетях могут быть очень изощренными и обеспечивать самые разные потребности пользователей в безопасном общении (телеконференции). Реализации таких схем приводят к появлению в сети специализированных серверов паролей.

В то же время парольная защита характеризуется определенными недостатками, связанными с особенностями психики.

Довольно часто пользователи, желающие облегчить себе жизнь, прикрепляют к терминалу компьютера, на котором установлена самая сложная парольная система разграничения доступа, листок с инструкцией, в котором описывается процедура вхождения в систему и приведен полный список паролей.

В связи с этим фирмы пытаются найти другие способы идентификации пользователя, не связанные с указанием пароля. Эти аппаратно-программные системы проверяют самые разные биометрические характеристики (подпись, узор линий на пальце, узор сосудов на глазном дне, манеру работать на клавиатуре) для того, чтобы обеспечить эффективные гарантии идентификации локального или удаленного пользователя.

На рынке СНГ представлены биометрическая система контроля доступа по отпечатку пальца американской фирмы *Identix* и биометрическая система контроля доступа по узору сетчатки глаза Eyedentify.

Большинство таких систем обладает тем недостатком, что они не отслеживают непрерывно во время работы неизменность биометрических характеристик пользователя, поэтому допускают в принципе временную подмену пользователя без какой-либо реакции со стороны системы защиты.

Конечно, определенные меры, затрудняющие подмену, принимаются: пользователь может "запереть" компьютер, отлучаясь ненадолго, для "отпирания" нужно знать специальный пароль; после определенного перерыва в непрерывной работе пользователь автоматически отключается от системы и для подключения ему нужно снова предъявлять свои полномочия.

Фирма *Electronic Signature Lock* из Орегона поставляет пакет программ ESL, который анализирует манеру пользователя работать на клавиатуре во время набора своего имени и пароля (парольная защита не исключается полностью).

Утверждается, что используемые статистические алгоритмы столь изощренны, что позволяют учитывать изменение этой манеры со временем, зависимость от состояния здоровья и т. д.

Фирма утверждает, что вероятность неверной идентификации пользователя, если он знает правильный пароль, менее од-

ной миллионной. Существует более совершенный вариант пакета CESL, который непрерывно отслеживает манеру пользователя работать на клавиатуре и может определить, когда за клавиатурой оказался не тот человек, что предъявлял полномочия на доступ.

После распознавания пользователя современная система должна выяснить, какие права предоставлены этому пользователю: какие данные он может использовать (читать, записывать, модифицировать, удалять); какие программы он может выполнять; когда, как долго и с каких терминалов он может работать и другие вопросы подобного рода.

В настоящее время существуют самые разные ***механизмы реализации разделения доступа (авторизации)***.

Одним из таких механизмов являются *"списки управления доступом"*. Смысл их состоит в том, что с каждым ресурсом системы при необходимости может быть сопоставлен соответствующий список, в котором указаны идентификаторы всех пользователей, которым разрешен (или, наоборот, запрещен) доступ к данному ресурсу, а также определено, какой именно доступ разрешен.

При обращении пользователя к данному ресурсу система автоматически проверяет наличие у данного ресурса списка управления доступом и при установлении его наличия проверяет, разрешено ли данному пользователю работать с данным ресурсом в запрошенном режиме.

В качестве ресурсов могут выступать как отдельные объекты системы (файлы, устройства, носители, программы и т. д.), так и целые компоненты системы (данные, устройства или программы) и даже вся система в целом.

Другим примером реализации механизма авторизации пользователя могут служить профили пользователей. *Профиль пользователя* — это организованный некоторым образом список, сопоставленный с определенным идентификатором пользователя и содержащий перечень всех объектов, к которым данному пользователю разрешен доступ, с указанием в каждом случае типа разрешенного доступа.

Существует также механизм, называемый матрицей доступа. *Матрица доступа* — это некоторая системная структура данных, которую легче всего представить в виде таблицы, столбцы которой помечены идентификаторами всех существующих в системе ресурсов, а строки — идентификаторами всех зарегистрированных в системе пользователей. На пересечении каждого столбца таблицы с каждой ее строкой администратором проставляется специальный указатель разрешенного данному пользователю типа доступа к данному объекту.

Для всех механизмов авторизации пользователя характерно следующее:

- доступ к данным механизмам должны иметь только специальные системные программы, обеспечивающие безопасность, а также строго ограниченный круг персонала системы, отвечающего за ее безопасность;
- указанные механизмы сами должны быть тщательно защищены от случайного или преднамеренного доступа к ним лиц или программ, не авторизованных для этого, поскольку эти механизмы являются одной из важнейших составляющих в обеспечении безопасности системы.

2.1.5. Выводы и рекомендации по защите информационных ресурсов фирмы

Защита информационной системы должна строиться по следующим основным направлениям:

1. *Защита аппаратуры и носителей информации от похищения, повреждения и уничтожения.*

Эта задача — часть общей проблемы защиты имущественных прав организаций. Для борьбы с угрозами этого вида используется традиционный комплекс организационно-технических мероприятий:

- физическая охрана и ограничение доступа к аппаратуре и носителям данных;
- ограждение зданий и территорий;
- оборудование помещений замками, охранной сигнализацией;

• использование различных устройств, препятствующих похищению компьютерной аппаратуры, ее компонентов и узлов.

2. *Защита информационных ресурсов от несанкционированного использования.* Для этого применяются средства контроля включения питания и загрузки программного обеспечения, а также методы парольной защиты при входе в систему.

3. *Защита информационных ресурсов от несанкционированного доступа.* Обеспечивает охрану конфиденциальности, целостности и готовности (доступности) информации и автоматизированных служб системы.

4. *Защита от утечки по побочным каналам электромагнитных излучений и наводок.* Реализуется экранированием аппаратуры и помещений, эксплуатацией специальной защищенной аппаратуры, применением маскирующих генераторов шумов и помех, а также дополнительной проверкой аппаратуры на наличие компрометирующих излучений.

5. *Защита информации в каналах связи и узлах коммутации.* Блокирует угрозы, связанные с пассивным подключением к каналу (подслушивание), предотвращает активное подключение с фальсификацией сообщений, а также препятствует блокировке каналов связи. Для защиты используются процедуры аутентификации абонентов и сообщений, шифрование и специальные протоколы связи.

6. *Защита юридической значимости электронных документов.* При передаче документов (платежных поручений, контрактов, распоряжений) по компьютерным сетям необходимо обеспечить доказательство истинности того, что документ был действительно создан и отправлен автором, а не сфальсифицирован или модифицирован получателем или каким-либо третьим лицом.

Кроме того, существует угроза отрицания авторства отправителем с целью снятия с себя ответственности за передачу документа. Для защиты от таких угроз в практике обмена финансовыми документами используются методы аутентификации сообщений при отсутствии у сторон доверия друг к другу.

Документ (сообщение) дополняется цифровой подписью — специальной меткой, неразрывно логически связанной с текстом и фор-

мируемой с помощью секретного криптографического ключа. Подделка таких меток без знания ключа посторонними лицами исключается и неопровержимо свидетельствует об авторстве. Нарушитель также не может отказаться от авторства документа.

7. *Защита автоматизированных систем от компьютерных вирусов и незаконной модификации.* Реализуется применением иммуностойких программ и механизмов обнаружения фактов модификации программного обеспечения.

При защите информации нужно соблюдать следующий принцип: если вы оцениваете информацию, скажем, в 1 млн руб., то тратить 100 млн руб. на ее охрану не стоит.

Американский опыт показывает, что защита информации — не только техническая, но и организационная проблема. Ключ к защите корпоративных данных — в информировании каждого сотрудника о мерах безопасности в масштабах всего предприятия.

Для того чтобы не пострадать от противоправной деятельности хакера, прислушайтесь к следующим рекомендациям:

1. Так как снять информацию с компьютера, оборудованного системой защиты, может только высококвалифицированный программист-системщик, при приеме на работу особое внимание уделяйте данной категории лиц. Желательно, чтобы их предварительно проверила служба безопасности вашей фирмы или частное сыскное бюро.

2. Не допускайте нового специалиста сразу ко всем программам до окончания проверки, даже если это принесет вам некоторые убытки.

3. Если у вас работает несколько программистов-системщиков, постарайтесь разделить их сферы влияния, организуйте работу по сменам, разнообразьте способы доступа к отдельным программам.

4. Поскольку программист — это прежде всего человек, не давайте побудительных мотивов к измене или инициативному шпионажу на вашей фирме. Программист — профессия высокооплачиваемая, его доход не должен быть меньше, чем на фир-

мах-конкурентах. Кроме того, меры социальной поддержки, моральное стимулирование, в том числе неформальная благодарность от руководства фирмы за проделанную работу в кругу сослуживцев, благотворно влияют на лояльность к фирме.

5. Стимулируйте у потенциальных хакеров дух творчества, давайте им возможность заработать на стороне за счет разработок игровых и учебных программ, преподавания в колледжах и школах. Иногда клин клином вышибают: предложите подозреваемому хакеру создать вирусную или защитную программу, и дух профессионализма уже не позволит ему работать против своего хозяина.

6. Не забывайте, что особую угрозу для безопасности информационных ресурсов представляют бывшие сотрудники компаний. Небрежность при увольнении или переводе сотрудников приводит к тому, что они в отместку могут обмануть самые лучшие системы защиты.

Единственного, самого надежного метода защиты информации не существует; как правило, используется та или иная комбинация методов защиты, которая и дает, с точки зрения администрации, приемлемые результаты. Более того, относительная непопулярность аппаратной защиты говорит о плохом соотношении "стоимость/надежность" для аппаратных средств.

И напротив, такие относительно дешевые, простые средства, как минимальная парольная защита, физическая изоляция компьютеров, сбор статистики работы, оказываются достаточными с точки зрения администраторов систем. При этом не надо забывать, что сама по себе парольная защита проблему безопасности не решает, но лишь создает иллюзию защиты.

В заключение отметим, что при защите информационных ресурсов имеет место трудноразрешимый компромисс между эффективностью и удобством компьютерной системы в работе и степенью обеспечения в ней требований безопасности. Чем более высокие требования предъявляются к безопасности системы, тем большее количество ресурсов системы затрачивается на обеспечение этих требований, тем сильнее снижается производительность системы

и увеличиваются сроки решения задач, наконец, тем неудобнее работать в данной системе пользователям.

С другой стороны, чем больше ресурсов выделяется для решения текущих задач, тем меньше возможностей по обеспечению должного уровня безопасности.

2.2. Защита информации при проведении совещаний и переговоров

Совещания и переговоры, в процессе которых могут обсуждаться сведения, составляющие тайну фирмы или ее партнеров, именуются обычно конфиденциальными. Порядок проведения подобных совещаний и переговоров регламентируется специальными требованиями, обеспечивающими безопасность ценной, в том числе конфиденциальной, информации (далее — ценной информации), которая в процессе этих мероприятий распространяется в санкционированном (разрешенном) режиме. Основной угрозой ценной информации является разглашение сведений о новой идее, продукции или технологии.

Причины, по которым информация может разглашаться на конфиденциальных совещаниях или переговорах, общеизвестны: слабое знание сотрудниками состава ценной информации и требований по ее защите, умышленное невыполнение этих требований, ошибки сотрудников, отсутствие контроля за изданием рекламной и рекламно-выставочной продукции и др.

Оглашение ценной информации в санкционированном режиме должно быть оправдано деловой необходимостью и целесообразностью для конкретных условий и характера обсуждаемых вопросов.

Основные этапы проведения конфиденциальных совещаний и переговоров — подготовка к проведению, процесс их ведения и документирования, анализ итогов и выполнения достигнутых договоренностей.

Разрешение на проведение конфиденциальных совещаний и переговоров с приглашением представителей других организаций и фирм дает исключительно первый руководитель фирмы.

Решение первого руководителя о предстоящем конфиденциальном совещании доводится до сведения референта, менеджера по безопасности информации, руководителя секретариата, секретаря, менеджера по конфиденциальной документации, управляющего делами фирмы и начальника службы безопасности.

В целях дальнейшего контроля за подготовкой и проведением такого совещания информация об этом решении фиксируется секретарем в специальной учетной карточке. В этой карточке указываются наименование совещания или переговоров, дата, время, состав участников по каждому вопросу, руководитель, ответственный за проведение, ответственный организатор, контрольные отметки, зона сведений о факте проведения, зона сведений по результатам совещания или переговоров.

Плановые и неплановые конфиденциальные совещания, проходящие без приглашения посторонних лиц, проводятся первым руководителем, его заместителями, ответственными исполнителями (руководителями, главными специалистами) по направлениям работы с обязательным предварительным информированием секретаря.

По факту этого сообщения референтом заводится учетная карточка описанной выше формы. Проведение конфиденциальных совещаний без информирования референта не допускается.

Доступ сотрудников фирмы на любые конфиденциальные совещания осуществляется на основе действующей в фирме разрешительной системы доступа персонала к конфиденциальной информации.

Приглашение на конфиденциальные совещания лиц, не являющихся сотрудниками фирмы, санкционируется только в случае крайней необходимости их личного участия в обсуждении конкретного вопроса. Присутствие их при обсуждении других вопросов запрещается.

Ответственность за обеспечение защиты ценной информации и сохранение тайны фирмы в ходе совещания несет руководитель, организующий данное совещание. Секретарь оказывает помощь руководителям и совместно со службой безопасности осуществля-

ет контроль за перекрытием возможных организационных и технических каналов утраты информации.

Подготовку конфиденциального совещания осуществляет организующий его руководитель с привлечением сотрудников фирмы, допущенных к работе с конкретной ценной информацией, составляющей тайну фирмы или ее партнеров.

Из числа этих сотрудников назначается ответственный организатор, планирующий и координирующий выполнение подготовительных мероприятий и проведение самого совещания. Этот сотрудник информирует референта о ходе подготовки совещания или переговоров. Полученная информация вносится секретарем в учетную карточку.

В процессе подготовки конфиденциального совещания составляются программа проведения совещания, повестка дня, информационные материалы, проекты решений и список участников совещания по каждому вопросу повестки дня.

Все документы, составляемые в процессе подготовки конфиденциального совещания, должны иметь гриф "Конфиденциально", изготовляться и издаваться в соответствии с требованиями инструкции по обработке и хранению конфиденциальных документов.

Документы (в том числе проекты договоров, контрактов и др.), предназначенные для раздачи участникам совещания, не должны содержать конфиденциальные сведения. Эта информация сообщается участникам совещания устно при обсуждении конкретного вопроса.

Цифровые значения наиболее ценной информации (технические и технологические параметры, суммы, проценты, сроки, объемы и т. п.) в проектах решений и других документах не указываются или фиксируются в качестве общепринятого значения, характерного для сделок подобного рода и являющегося стартовой величиной при обсуждении.

В проектах не должно быть развернутых обоснований предоставляемых льгот, скидок или лишения льгот тех или иных партнеров, клиентов. Документы, раздаваемые участникам совещания, не должны иметь грифа конфиденциальности.

Список участников конфиденциального совещания составляется отдельно по каждому обсуждаемому вопросу. К участию в обсуждении вопроса привлекаются только те сотрудники фирмы, которые имеют непосредственное отношение к этому вопросу. Это правило касается и руководителей.

В списке участников указываются фамилии, имена и отчества лиц, занимаемые должности, представляемые ими учреждения, организации, фирмы и наименования документов, подтверждающих их полномочия вести переговоры и принимать решения. Название представляемой фирмы может при необходимости заменяться ее условным обозначением.

Документом, подтверждающим полномочия лица (если это не первый руководитель) при ведении переговоров и принятии решений по конкретному вопросу, могут служить письмо, предписание, доверенность представляемой лицом фирмы, рекомендательное письмо авторитетного юридического или физического лица, письменный ответ фирмы на запрос о полномочиях представителя, в отдельных случаях — телефонное или факсимильное подтверждение полномочий первым руководителем представляемой фирмы.

Эти документы передаются участниками совещания ответственному организатору непосредственно перед началом совещания для последующего включения их референтом в дело, содержащее все материалы по данному совещанию или переговорам.

Документы, составляемые при подготовке конфиденциального совещания, на котором предполагается присутствие представителей других фирм и организаций, согласовываются с референтом и руководителем службы безопасности. Отмеченные ими недостатки в обеспечении защиты ценной информации должны быть исправлены ответственным организатором совещания. После этого документы утверждаются руководителем, организующим совещание.

Одновременно с визированием подготовленных документов референт, руководитель службы безопасности и ответственный организатор определяют место проведения совещания, порядок доступа участников совещания в это помещение, порядок докумен-

тирования хода обсуждения вопросов и принимаемых решений, а также порядок рассылки (передачи) участникам совещания оформленных решений и подписанных документов.

Любое конфиденциальное совещание организуется в специальном (выделенном) помещении, имеющем лицензию на проведение подобного мероприятия и, следовательно, оборудованном средствами технической защиты информации. Доступ в такие помещения сотрудников фирмы и представителей других фирм и организаций разрешается руководителем службы безопасности.

Перед началом конфиденциального совещания сотрудники службы безопасности обязаны убедиться в отсутствии в помещении несанкционированно установленных аудио- и видеозаписывающих или передающих устройств, убедиться в качественной работе средств технической защиты на всех возможных каналах утечки информации.

Помещение должно быть оборудовано кондиционером, так как открытие окон, дверей в ходе совещания не допускается. Окна закрываются шторами, входная дверь оборудуется сигналом, оповещающим о ее неплотном закрытии. В целях звукоизоляции целесообразно иметь двойную дверь (тамбур) или зашторивать двери звукопоглощающей тканью.

Проведение совещания в неприспособленных и не оборудованных соответствующим образом помещениях фирмы (кроме кабинета первого руководителя) не разрешается.

В помещении для проведения конфиденциальных совещаний не должны находиться приборы, оборудование и технические средства, которые непосредственно не используются для обеспечения хода совещания (например, телефоны городской сети, ПК, телевизионные и радиоприемники и др.).

При необходимости они размещаются в соседней, изолированной комнате. Аудио- и видеозапись конфиденциальных совещаний, фотографирование ведутся только по письменному указанию первого руководителя фирмы и осуществляются одним из сотрудников фирмы, готовивших совещание.

Чистый носитель информации для этих целей выдается референтом под роспись в учетной форме и возвращается ему с зафик-

сированной информацией по окончании каждого дня работы совещания.

Доступ участников конфиденциального совещания в помещение, в котором оно будет проводиться, осуществляет ответственный организатор совещания под контролем сотрудника службы безопасности в соответствии с утвержденным списком и предъявляемыми участниками персональными документами.

Перед началом обсуждения каждого вопроса состав присутствующих корректируется. Нахождение (ожидание) в помещении лиц, в том числе сотрудников данной фирмы, не имеющих отношения к обсуждаемому вопросу, не разрешается.

Целесообразно, чтобы при открытии совещания организовавший его руководитель напомнил участникам о необходимости сохранения производственной и коммерческой тайны, уточнил, какие конкретные сведения являются конфиденциальными на данном совещании.

Ход конфиденциального совещания документируется одним из готовивших его сотрудников или секретарем-стенографисткой. На закрытых совещаниях с повышенным уровнем конфиденциальности эту работу выполняет непосредственно ответственный организатор совещания. Составляемый протокол (стенограмма) должен иметь гриф конфиденциальности необходимого уровня и оформляться в стенографической тетради, зарегистрированной секретарем.

Целесообразность записи хода совещания участниками определяет руководитель, организовавший совещание, исходя из содержания информации, которая оглашается. Руководитель имеет право не разрешить участникам совещания вести какие-либо записи или санкционировать ведение этих записей на листах бумаги, зарегистрированных референтом, с последующей сдачей их этому лицу и доставкой курьерами фирмы по месту работы участников совещания.

При необходимости вызова на проходящее совещание дополнительных лиц (экспертов, консультантов, представителей других фирм и организаций) факт их участия в совещании фиксируется в протоколе с указанием мотивов вызова. Присутствие этих лиц на

совещании ограничивается временем рассмотрения той ситуации, по которой они были вызваны.

Участникам конфиденциального совещания, независимо от занимаемой должности и статуса на совещании, не разрешается:

• вносить в помещение, в котором проводится совещание, фото, кино- и видеоаппаратуру, компьютеры, плейеры, диктофоны и другую аппаратуру, пользоваться ею;

• делать выписки из документов, используемых при решении вопросов на совещании и имеющих гриф ограничения доступа;

• обсуждать вопросы, вынесенные на совещание, в местах общего пользования;

• информировать о совещании (вопросах повестки дня, составе участников, времени и месте проведения, ходе обсуждения вопросов, содержании решений и т. п.) любых лиц, не связанных с проведением данного совещания, в том числе сотрудников фирмы.

Участники совещания, замеченные в несанкционированной аудио- или видеозаписи, использовании средств связи, фотографировании, лишаются права дальнейшего присутствия на совещании. По данному факту составляется акт, копия которого направляется фирме, представителем которой является данное лицо, или передается первому руководителю фирмы — организатора совещания, если это лицо является сотрудником последней. Одновременно носитель несанкционированно записанной информации передается референту для учета и хранения (или уничтожения). Устройство записи возвращается владельцу.

Участники совещания не могут оглашать больший объем ценных сведений, чем это было установлено при подготовке совещания, или сообщать сведения, не относящиеся к обсуждаемому вопросу. Состав оглашаемых сведений регламентируется руководителем, организовавшим совещание.

По окончании конфиденциального совещания сотрудник службы безопасности осматривает помещение, запирает, опечатывает и сдает под охрану.

Документы, принятые на совещании, оформляются, подписываются, при необходимости размножаются и рассылаются (передаются) участникам совещания в соответствии с требованиями по работе с конфиденциальными документами фирмы. Все экземпляры этих документов должны иметь гриф ограничения доступа. Рассылать документы, содержащие строго конфиденциальную информацию, не разрешается.

При проведении ***переговоров по заключению, продлению или прекращению*** какого-либо ***договора (контракта)*** должны соблюдаться некоторые дополнительные требования, соблюдение которых контролирует референт.

В процессе подготовки переговоров первоначально необходимо выяснить намерения организации или фирмы, с которой предполагаются переговоры. Если это малоизвестная фирма, то целесообразно получить о ней подробную информацию, чтобы избежать ошибочного выбора партнера или клиента.

Подготовительная работа по проведению переговоров предполагает выработку плана переговоров и определение на этой основе дозированного состава ценной информации, которую допускается использовать в общении с участниками переговоров, порядка ее оглашения и условий возникновения в этом рабочей необходимости.

Сообщаемые на этом этапе сведения не должны содержать производственной или коммерческой тайны. Сотрудникам фирмы, участвующим в переговорах, не разрешается использовать в дискуссии конфиденциальную информацию и раскрывать желаемые результаты переговоров, итоги аналогичных переговоров с другими партнерами. В процессе неофициальной части переговоров обсуждение вопросов, связанных с содержанием и ходом дискуссии, не допускается.

При ведении переговоров не следует сразу же передавать партнеру всю запрашиваемую им информацию в полном объеме. Прежде всего следует выяснить, для какой цели ему необходимы эти сведения и как знание этих сведений отразится на ходе дальнейшего сотрудничества с ним.

На этом этапе переговоров, при выяснении сути взаимных намерений, целесообразно строить дискуссию таким образом, чтобы

ответы на вопросы были максимально лаконичными ("да — нет", "можем — не можем"). Однако после юридического оформления взаимоотношений и подписания партнерами, клиентами обязательства о неразглашении ценных сведений они могут быть более подробно ознакомлены с предметом договора.

В договоре по итогам переговоров должно найти отражение взаимное обязательство сторон о защите ценных и особенно конфиденциальных сведений, недопустимости передачи их без предварительного согласия сторон третьему лицу, необходимости ознакомления с предметом договора ограниченного числа сотрудников, которые предварительно должны подписать обязательства о сохранении в тайне полученных сведений.

В коммерческой практике местом проведения переговоров часто становятся постоянно действующие и периодические торговые или торгово-промышленные ***выставки и ярмарки***. Секретарь должен знать порядок защиты ценной информации фирмы в ходе этих переговоров, инструктировать их участников и контролировать соблюдение ими установленных правил.

Любая выставка является, с одной стороны, отличным источником полезной для бизнеса информации, объектом добросовестного маркетингового исследования рынка товаров, а с другой — опасным каналом несанкционированного получения конфиденциальных сведений, касающихся новых идей, технологий и продукции.

Обобщенно источники ценных сведений в процессе выставочной деятельности включают в себя экспозицию, персонал фирмы, участвующий в выставке, и рекламно-выставочные материалы.

Утрата ценной информации происходит вследствие общения специалистов родственных профессий, но разных фирм и наличия в выставочной экспозиции самого нового продукта. Проводимые параллельно с выставочными мероприятиями пресс-конференции, семинары, презентации фирм и товаров создают дополнительную угрозу сохранности ценной информации.

Работа персонала фирмы с посетителями выставки должна быть строго регламентирована, прежде всего в части состава огла-

шаемых сведений о продукции, технических и технологических новшествах, заключенных в этой продукции. Обязательно учитывается, что состав этих сведений дифференцируется в зависимости от категории посетителей — массового посетителя-дилетанта ("любителя") и посетителя — специалиста в данной области ("эксперта").

Целесообразно использовать метод "черного ящика", при котором посетителю сообщается все, что касается назначения продукции и ее потребительских качеств, но остаются в тайне технология и способы, которыми достигнуты эти качества, функциональные возможности продукции.

Поэтому персоналу, обслуживающему экспозицию фирмы, должны быть недоступны сведения о продукции, отнесенные к производственной или коммерческой тайне. В свою очередь, специалисты фирмы, осведомленные о ее секретах, не должны участвовать в работе выставочного стенда.

Объясняется это тем, что специалист в процессе дискуссии с посетителем может увлечься и сообщить больший объем сведений, чем это предусмотрено. Не допускается знакомить посетителей, клиентов и партнеров с изобретателями, конструкторами, технологами, работающими над новыми идеями и новой продукцией.

Рекламно-выставочные материалы (проспекты, пресс-релизы, прайс-листы, брошюры и т. п.) следует рассматривать как контролируемый канал распространения ценных сведений. При этом следует помнить, что этот канал тщательно и глубоко анализируется конкурентом с целью выявления тех сведений, которые составляют тайну фирмы, издавшей рекламные материалы.

Защита информации в рекламно-выставочной деятельности предусматривает заблаговременный анализ, экспертизу любой предназначенной для широкого оглашения информации о деятельности фирмы и ее продукции.

Подобная информация должна, как правило, анализироваться от противного — с точки зрения того интереса, который будет проявлен к ней конкурентами, и объема полезных сведений, извлекаемых конкурентом из ее содержания.

Материалы, не прошедшие экспертизу, публикации не подлежат. Экспертиза включает также последующий контроль всех опубликованных о фирме материалов, сообщений средств массовой информации, рекламных изданий и рекламно-выставочных проспектов.

Помимо этого, анализируются подобные материалы других фирм для определения возможной утраты ценных сведений. Рекламно-выставочные издания не должны сигнализировать недобросовестному конкуренту о том, что и где искать.

Чтобы предотвратить разглашение ценных сведений в рекламно-выставочных материалах, следует заблаговременно:

• проанализировать множество предполагаемых к изданию и изданных материалов с точки зрения возможности извлечения из них ценных конфиденциальных сведений;

• осуществить разбиение (дробление) информации на части и распределение их между разными рекламно-выставочными материалами, предназначенными для массового посетителя и посетителей-специалистов, издать серию дополнений к основному проспекту для специалистов разного профиля;

• осуществить разбиение информации по видам и средствам рекламы — традиционным бумажным изданиям, электронной рекламе, веб-странице, рекламе в средствах массовой информации и др.

Вместе с тем, должен соблюдаться разумный баланс: рекламно-выставочные материалы не должны быть малоинформативными для посетителей, все наиболее важные параметры новой продукции должны найти в них отражение.

Таким образом, подготовка и проведение совещаний и переговоров по конфиденциальным вопросам, оформление их результатов связаны с выполнением ряда обязательных процедур, необходимых для правильной организации работы организаторов и участников этих мероприятий.

При несоблюдении изложенных требований возникает серьезная опасность разглашения или утечки ценных сведений и секретов фирмы, ее партнеров и клиентов. Контроль за выполнением этих требований возлагается на секретаря, который обеспечивает информацион-

ную безопасность деятельности фирмы, сохранение ее деловых и производственных секретов.

2.3. Защита информации при работе с посетителями

Организация приема посетителей имеет не только общеизвестный набор функций, но и другую, менее изученную, но актуальную сторону, затрагивающую сферу обеспечения информационной безопасности деятельности фирмы при работе с посетителями.

Профессионализм персонала фирмы предполагает умение организовать эффективную и полезную для фирмы работу с посетителями и одновременно выполнить ее таким образом, чтобы была сохранена конфиденциальность и целостность ценной информации, достигнута безопасность деятельности фирмы.

Под посетителем понимается, во-первых, лицо, которому необходимо решить определенный круг деловых или личных вопросов с руководителями и менеджерами фирмы, и, во-вторых, лицо, совместно с которым полномочные лица вырабатывают определенные решения по направлениям деятельности фирмы.

Посетители не только по определению, но и по существу представляют собой сложный и неоднозначный круг людей, что требует прежде всего грамотного решения вопросов защиты ценной, в том числе конфиденциальной, информации от угроз, которые могут создать ей посетители.

Поэтому организацию приема посетителей и контроль за работой с ними следует централизовать на уровне секретаря первого руководителя фирмы. Работа именно этого сотрудника фирмы в наибольшей степени связана с посетителями и требует грамотного подхода к ее выполнению.

Процесс защиты информации при приеме посетителей предполагает проведение четкой их классификации, на базе которой формируется система ограничительных, технологических, контрольных и аналитических мер, призванных не допустить несанкционированный доступ к ценной информации. Эти меры позво-

ляют также в определенной степени гарантировать физическую безопасность сотрудников, работающих с посетителями.

Прием посетителей и установление с ними деловых взаимоотношений — достаточно сложный процесс для руководителей фирмы и ее структурных подразделений, специалистов-менеджеров.

На уровне руководителей фирмы посетителей можно разделить на две категории: сотрудники фирмы и посетители, не являющиеся ее сотрудниками.

К посетителям — сотрудникам фирмы относятся:

1) сотрудники, имеющие право свободного входа в кабинет руководителя в любое время рабочего дня (заместители руководителя, референты, секретари);

2) сотрудники, работающие с руководителем в режиме вызова или решающие с ним деловые вопросы в часы приема по служебным делам (нижестоящие руководители, эксперты, специалисты-менеджеры);

3) сотрудники, приходящие на прием по личным вопросам.

Угрозы информационной безопасности, исходящие от посетителей-сотрудников, могут наступить в случае, если эти сотрудники являются злоумышленниками (тайными представителями конкурирующих фирм, агентами служб промышленного или экономического шпионажа, криминальных структур) или их сообщниками.

Состав угроз может быть самым разнообразным: от кражи документов со стола руководителя до выведывания нужной информации с помощью хорошо подготовленного перечня, на первый взгляд, безобидных вопросов. Может случиться также, что сотрудник, получивший при общении с руководителем больший объем ценной информации, чем это необходимо ему для работы, разглашает ее постороннему лицу по причине элементарной безответственности.

Посетители, не являющиеся сотрудниками фирмы, в соответствии с характером их взаимоотношений с фирмой могут подразделяться на следующие категории:

1) лица, не включенные в штат сотрудников, но входящие в качестве членов в коллективный орган управления деятельностью фирмы (акционеры, члены различных советов и др.);

2) представители государственных учреждений и организаций, с которыми фирма сотрудничает в соответствии с законом (работники различных инспекций, муниципальных органов управления, правоохранительных органов и др.);

3) сотрудничающие с фирмой физические лица и представители предприятий и организаций, банков, рекламных агентств, торговых представительств, средств массовой информации (клиенты, партнеры, коммерсанты, инвесторы, спонсоры, журналисты и др.);

4) представители иных государственных и негосударственных структур, с которыми фирма не имеет деловых отношений;

5) частные лица.

Перечисленные представители и лица должны находиться под особо внимательным контролем референта, так как если они относятся к категории злоумышленников, спектр исходящей от них опасности крайне велик и определяется теми целями, которые перед ними поставлены.

Утрата информации может идти по организационным или техническим каналам или в их сочетании. Например: шантаж руководителя и запись беседы на диктофон, установка подслушивающего устройства, фотографирование документов на столе руководителя и др. Не исключено силовое воздействие на руководителя в целях получения нужных сведений.

На уровне руководителей подразделений и специалистов-менеджеров фирмы выделяются аналогичные группы посетителей, но в каждой категории и группе посетители подразделяются на направленных руководителем и пришедших на прием без санкции руководителя.

При приеме руководителем фирмы любой из указанных категорий и групп посетителей следует соблюдать следующие **основные правила организации приема**.

Руководитель не должен принимать посетителей во время, выделенное для творческой работы с документами и базами электронных данных, особенно конфиденциальными.

При вызове кого-либо из менеджеров в связи с работой над документом на столе руководителя должен находиться только тот документ, с которым он работает, другие документы следует хранить в запертом сейфе или металлическом шкафу. Целесообразно, чтобы в это время в кабинет руководителя никто не заходил без вызова, в том числе и лица, имеющие право свободного входа в кабинет.

Для приема посетителей любых категорий следует выделить специальные часы, в течение которых руководитель не должен работать с документами, не относящимися к визиту того или иного лица, или вести деловые переговоры по телефону. Различные категории посетителей целесообразно принимать в разные часы.

Во-первых, выделяется время для ежедневного приема нижестоящих руководителей и менеджеров фирмы по служебным вопросам.

Во-вторых, выделяется время для ежедневного приема посетителей, не являющихся сотрудниками фирмы, но представляющих ту или иную организационную структуру.

В-третьих, отдельные часы приема выделяются в разные дни для частных (посторонних) лиц, которым необходимо решить вопрос, относящийся к компетенции руководителя. В часы приема указанных категорий посетителей любые сотрудники фирмы могут посещать руководителя только по вызову и только по вопросу, связанному с визитом конкретного посетителя.

В-четвертых, периодически выделяются часы приема сотрудников фирмы по личным вопросам.

Посетители, в том числе сотрудники фирмы, не должны входить в кабинет руководителя в пальто, шубе или иметь при себе объемные кейсы, чемоданы, сумки — их следует оставлять в приемной.

Не допускается оставлять посетителя одного при выходе руководителя из кабинета. Во время отсутствия руководителя никто из посетителей или персонала фирмы не должен входить в его кабинет.

Наиболее тщательно должна быть организована ***работа секретаря с посетителями, которые не являются сотрудниками фирмы.***

Следует учитывать, что посещение руководителя, как правило, является начальной стадией их визита в фирму. Другие стадии, в соответствии с решением руководителя, будут связаны с посещением нижестоящих руководителей и специалистов-менеджеров.

С точки зрения обеспечения информационной безопасности фирмы таких посетителей можно классифицировать следующим образом:

• по степени разрешенного им доступа в помещения фирмы: во все помещения; только в определенные помещения; только к определенному сотруднику; только в операционный зал общего доступа;

• по степени разрешенного им ознакомления с информацией фирмы: только с рекламными изданиями; только с материалами, касающимися заинтересованной структуры или лица; только с материалами по определенному вопросу; только с открытыми служебными материалами фирмы; только с конкретными конфиденциальными сведениями.

Любые разрешительные действия в отношении посетителей совершаются первым руководителем фирмы и контролируются при реализации службой безопасности.

Работа с посторонним посетителем состоит из следующих этапов:

1. Подготовительного этапа.

2. Идентификации и регистрации посетителя.

3. Организации приема посетителя руководителем.

4. Организации дальнейших действий посетителя.

1. *Подготовительный этап* включает согласование возможности и условий приема посетителя руководством или сотрудником фирмы. Визит, как правило, инициируется самим посетителем и должен быть заранее обсужден им по телефону, электронной почте или факсу с руководителем или референтом, а также с менеджером, если посетитель предполагает решить с ним возникший вопрос.

В процессе согласования визита выясняется цель предполагаемого посещения фирмы, состав необходимых для ознакомления документов, дата и время посещения. Визит к руководителю предполагает, что посетителю необходимо решить вопрос, вхо-

дящий в компетенцию этого должностного лица, или при необходимости получить санкцию руководителя на выполнение определенной работы в подразделении фирмы и ознакомление с документами, базами данных.

В других случаях посетителя следует направить к специалисту-менеджеру, в компетенцию которого входит рассмотрение интересующего посетителя вопроса.

По результатам согласования уточняется должностное лицо фирмы, которое вправе решить поставленный посетителем вопрос, корректируются дата и время визита. После согласования фамилия, имя, отчество посетителя, наименование представляемой организационной структуры и указанные выше сведения вносятся в график приема посетителей фирмы.

Составление, уточнение и дополнение графика приема посетителей является обязанностью референта. График согласовывается референтом с руководителями и специалистами-менеджерами в начале предыдущего рабочего дня. О намеченном визите и часах приема напоминается будущему посетителю.

Ежедневное число посетителей должно соответствовать реальному времени, отведенному руководителем или менеджером на этот вид работы.

В часы приема каждой из категорий и групп посетителей важно четко определить период нахождения каждого посетителя в приемной и кабинете руководителя или на рабочем месте менеджера, для чего устанавливаются очередность приема и предполагаемая продолжительность переговоров.

Сложные и длительные по времени вопросы обсуждаются в первую очередь. Особенно четко должен регламентироваться прием лиц, не являющихся сотрудниками фирмы.

Следует планировать прием таким образом, чтобы посетители длительное время не находились в приемной, так как подобные ожидания всегда сопровождаются подсознательным или умышленным прослушиванием переговоров в приемной, получением значительного объема ценной информации. Не допускается организовывать так называемую живую очередь.

График целесообразно формировать централизованно в виде единой схемы, охватывающей посетителей руководства фирмы

и структурных подразделений. Руководители подразделений и менеджеры обязаны ежедневно сообщать референту о согласованных с ними визитах посетителей для включения фамилий в график приема.

Это позволяет обеспечить высокую достоверность включаемых в график сведений и контролировать обоснованность визитов посетителей на уровне подразделений фирмы.

В помещениях фирмы не должны находиться посторонние лица, относящие себя к категории посетителей, хотя их визит не был согласован и зафиксирован в графике приема.

На основании графика референт ежедневно в начале рабочего дня сообщает сведения о посетителях и характере разрешенного из доступа к делам фирмы в службу безопасности для оформления пропусков. Пропуск может оформляться только по инициативе референта.

Одновременно референт напоминает сотрудникам структурных подразделений фамилии посетителей, визит которых намечен на текущий день, и время приема.

При изменении даты визита необходимое исправление вносится в график приема посетителей, а посетитель в обязательном порядке заблаговременно информируется об этом. С ним согласовывается новая дата визита и время.

2. *Идентификация*, т. е. установление соответствия личности посетителя сведениям в графике приема и документе, удостоверяющем его личность, выполняется на двух уровнях:

1) сотрудником службы безопасности при входе в здание фирмы и выдаче посетителю пропуска;

2) секретарем при входе посетителя в приемную руководителя фирмы.

На первом уровне идентифицируется личность посетителя и соответствие фамилии, имени, отчества записи в переданном референтом в службу безопасности перечне посетителей на конкретный день и час.

При входе в помещение фирмы (кроме операционного зала общего доступа) посетитель обязан предъявить сотруднику службы

безопасности паспорт или служебное удостоверение, подтверждающие его личность (но не визитную карточку).

Особое внимание обращается на выявление подлинности предоставленного персонального документа и установление соответствия фотокарточки в этом документе внешним данным посетителя.

После идентификации посетителю выдается подготовленный заранее соответствующий визуальный идентификатор (пропуск), регламентирующий его права в помещениях фирмы.

Перемещение посетителя в здании осуществляется только в сопровождении работника фирмы — секретаря, менеджера, с которым посетитель обговорил свой визит, сотрудника службы безопасности.

Все посетители фирмы, в том числе посетители структурных подразделений, сначала направляются к референту с целью их идентификации и регистрации. Войдя в приемную руководства фирмы, посетитель должен предъявить референту удостоверяющий его личность документ и предписание.

Идентификация посетителя на втором уровне предполагает проверку соответствия его личности, места работы и должности сведениям, указанным в графике приема. При возникновении каких-либо сомнений в личности посетителя референт может уточнить сведения о нем в организации, которую представляет данное лицо (по телефону, электронной почте).

Если сомнения не устранены, референт должен получить разрешение на доступ данного посетителя в кабинет руководителя или структурное подразделение от начальника службы безопасности фирмы.

После завершения этапа идентификации секретарь на основе предоставленных документов вносит сведения о посетителе в традиционный или электронный журнал учета (регистрации) посетителей. Указываются: дата и время приема, фамилия, имя, отчество посетителя, место работы и должность, наименование вопроса, исходные данные предписания, фамилия сотрудника фирмы, ответственного за визит, принятое решение. Группа посетителей, прибывшая для переговоров, регистрируется пофамильно. Записи делаются в журнале лично секретарем.

Не допускается, чтобы посетитель знакомился со сведениями в графике приема и журнале регистрации посетителей, так как информация, включаемая в эти учетные формы, является конфиденциальной, раскрывающей деловые связи фирмы.

3. *Организация приема посетителя.* После регистрации посетители структурных подразделений направляются по назначению в сопровождении встретивших их секретарей или менеджеров, а посетители руководителей фирмы остаются в приемной, и референт приступает к организации их приема руководителем.

Ожидающий приема посетитель должен находиться на значительном расстоянии от рабочего места секретаря, чтобы он не мог видеть документы, находящиеся на столе, экран дисплея, прослушивать переговоры по средствам связи.

Холл для ожидающих приема посетителей может отделяться от рабочего места секретаря стеклянной тонированной перегородкой.

При приеме посетителей секретарю не разрешается покидать помещение приемной даже на непродолжительное время. Переговоры с руководителем ведутся им по соответствующему коммуникативному устройству.

В период ожидания посетителем приема секретарю целесообразно внимательно наблюдать за его поведением, фиксировать возможные странности в движениях, излишнюю возбужденность и т. п. Под особым контролем секретаря должна находиться группа посетителей, ожидающих приема для переговоров по одному вопросу (заключение контракта, получение согласия на выполнение определенной работы и др.).

При возникновении каких-либо опасений секретарь должен вызвать сотрудника службы безопасности, который будет присутствовать в кабинете при беседе руководителя с посетителем или посетителями.

Сотруднику этой службы не следует быть в традиционной униформе подразделения охраны, внешне он не должен отличаться от других работников фирмы.

При приеме частных (иногда случайных) лиц руководитель может вести беседу не в рабочем кабинете, а в специально пред-

назначенном для этого помещении, в присутствии сотрудника службы безопасности.

Переговоры руководителя с посетителем могут документироваться секретарем-стенографисткой или записываться на магнитный носитель с помощью диктофона, видеокамеры.

Посетитель — представитель другой организационной структуры предъявляет руководителю предписание, в котором указываются его полномочия, цель и задачи визита в данную фирму, состав сведений и документов, которые ему необходимы для ознакомления или анализа. Представление оформляется на бланке организации, подписывается ее первым руководителем, подпись руководителя заверяется печатью.

На предписании руководитель фирмы пишет резолюцию, в которой дает разрешение посетителю на выполнение стоящих перед ним задач, устанавливает порядок и сроки его работы, регламентирует конкретный состав информации, к которой может быть допущен посетитель, назначает сотрудника фирмы, функциональные обязанности которого соответствуют цели визита посетителя, ответственным за работу с этим лицом.

Руководитель имеет право не давать разрешения или ограничить характер работы посетителя в фирме.

Устные пожелания посетителя, не имеющего предписания, и пожелания, не устраивающие руководителя, выполняться не должны.

Прием посетителя или группы посетителей может иметь форму переговоров, например, о поставках продукции, финансовой помощи, совместных исследованиях и по другим вопросам. В переговорах могут участвовать сотрудники фирмы, состав которых был заранее определен и внесен в график приема. Ход переговоров обычно фиксируется секретарем-стенографисткой.

Прием посетителей (групп посетителей, делегаций) может также иметь форму экскурсий по фирме (предприятию) с целью ознакомления с возможностями фирмы и применяемыми прогрессивными технологиями. В этом случае заблаговременно определяется маршрут движения группы, состав объектов для ознакомления, готовится и издается иллюстративный материал (проспекты, видеофильмы, веб-страницы и др.).

Программа пребывания группы посетителей на территории фирмы должна сочетать максимальное гостеприимство и высокую степень ограничения в передаче посетителям дозированной информации о производственных и деловых процессах. Лаборатории, исследовательские центры демонстрироваться посетителям не должны.

4. По окончании приема руководителем референт *организует дальнейшие действия посетителя*: посетитель в сопровождении сотрудника службы безопасности направляется к выходу из здания или в приемную секретаря руководителя подразделения фирмы или специалиста-менеджера, к которым посетитель направлен для решения важных для него задач, в том числе содержащихся в предписании.

Секретарь вносит необходимое дополнение в пропуск-идентификатор посетителя, заверяя сделанную запись штампом приемной. Соответствующая запись делается в журнале регистрации посетителей. При необходимости секретарь предупреждает посетителя о недопустимости разглашения полученных во время визита сведений.

Целесообразно, чтобы посетитель подписал письменное обязательство о сохранении в тайне секретов фирмы. Одновременно секретарь напоминает руководителю подразделения или менеджеру о порядке предоставления посетителю минимально необходимого состава документов и сведений.

Предписание передается секретарем лицу, сопровождающему посетителя, для использования в работе и включения в дело; посетителю оно не возвращается. При отрицательном решении руководителя предписание передается им референту для включения в соответствующее дело.

Сведения о посетителях, работа которых в здании фирмы будет продолжаться несколько дней или во внерабочее время, вносятся секретарем в специальный журнал учета работы посетителей. Одновременно эти сведения сообщаются в службу безопасности для выдачи посетителю необходимого пропуска-идентификатора и контроля за его пребыванием в здании фирмы.

В журнале службы безопасности ежедневно делаются отметки о времени прихода и ухода посетителя.

По истечении часов приема посетителей любой категории кабинет руководителя осматривается сотрудником службы безопасности в присутствии секретаря с целью обнаружения забытых посетителями вещей, документов, выявления возможно установленных посетителями подслушивающих и записывающих устройств, взрывных, химических и самовозгорающихся материалов и т. п.

В подразделениях фирмы соблюдается в целом тот же порядок приема и работы с посетителями.

Посетителю, направленному в подразделение вышестоящим руководителем, с учетом занятости руководителя подразделения или менеджера может быть назначен другой день приема. Однако более правильно организовать работу посетителя таким образом, чтобы в течение одного визита в фирму он смог решить все необходимые задачи.

Посетитель может быть допущен только к тем документам, сведениям, которые указаны в предписании и работа с которыми ему разрешена в резолюции руководителя. Ознакомление с документами осуществляется в присутствии сотрудника подразделения, назначенного в резолюции ответственным за выполнение посетителем порученного ему задания.

Записи и выписки, которые делает посетитель, могут выполняться на учтенном секретарем носителе и затем пересылаться с курьером по месту работы посетителя.

Факт ознакомления посетителя с любым конфиденциальным или открытым документом фирмы фиксируется в учетной форме этого документа.

На самом документе посетитель ставит визу ознакомления, расшифровку росписи, наименование организации и дату.

Не разрешается знакомить посетителя с документами и другими информационными ресурсами фирмы, даже если они связаны с целью его визита, без письменной санкции первого руководителя фирмы. В устных беседах с посетителем запрещается сообщать ему открытые или конфиденциальные сведе-

ния, которые не оговорены в резолюции руководителя, делать намек на наличие таких сведений.

Все перемещения посетителя в здании фирмы осуществляются в строгом соответствии с выданным ему идентификатором, желательно — в сопровождении менеджера или секретаря. Наблюдение за передвижением и работой посетителя может быть организовано с помощью видеокамер. Бесконтрольное пребывание посетителя в здании фирмы не допускается.

Посетители, нарушившие правила работы с информационными ресурсами фирмы, замеченные в попытке проникновения в другие помещения фирмы или несанкционированного получения ценных сведений у персонала, лишаются права дальнейшего пребывания в здании фирмы.

По окончании работы в структурном подразделении посетитель покидает здание в сопровождении сотрудника службы безопасности. При выходе посетитель сдает идентификатор (пропуск).

Посетитель-злоумышленник может использовать доступ в здание фирмы в криминальных целях, для создания определенной, выгодной ему экстремальной ситуации.

В числе основных видов подобных ситуаций, которые может провоцировать посетитель, следует назвать следующие: поджог или задымление помещений с целью ограбления, овладения документами, делами, очными вещами сотрудников; захват сотрудников в заложники; угроза физического насилия с целью выведать у сотрудника нужные сведения, получить документы, материальные ценности и др.

Самостоятельная ликвидация указанных экстремальных ситуаций силами работников службы безопасности не разрешается, так как требует специальных знаний, умений и осуществляется правоохранительными и противопожарными органами.

Чтобы предотвратить возникновение по вине посетителей той или иной экстремальной ситуации, персонал фирмы должен неукоснительно соблюдать указанные выше требования безопасности при приеме посетителей и работе с ними.

Всегда целесообразнее предупредить экстремальную ситуацию, чем ликвидировать ее последствия. Важно, чтобы персонал фирмы был заблаговременно обучен выполнению необходимых действий в случае возникновения конкретной экстремальной ситуации. У каждого сотрудника должна сложиться система устойчивых стереотипов (мотиваций) поведения в неординарных условиях.

Разработка системы противодействия злоумышленнику и обучение сотрудников возлагаются на службу безопасности. Система предусматривает классификацию экстремальных ситуаций для конкретной фирмы, систематическое проведение учебных занятий для должностных групп персонала, работающих с посетителями, обучение нормам поведения в том или ином случае, разработку схемы оповещения персонала об опасности и вступлении в действие плана эвакуации документов, дел, ценного оборудования, разработку схемы оповещения правоохранительных и противопожарных органов и служб, схемы эвакуации персонала в безопасную зону и др.

Обучение персонала должно включать изучение нормативных и плановых документов, решение ситуационных задач и проведение регулярных деловых игр. Большое значение имеет не только наличие необходимых нормативных и плановых документов, схем, программ обучения и инструктирования сотрудников, но и инженерно-техническое обеспечение действий персонала.

Здесь следует отметить необходимость функционирования в здании фирмы современных средств оповещения: о возгораниях, задымлении, нападении на сотрудника и т. п. Например, при приеме посетителей руководитель и секретарь должны располагать исправной сигнализацией для вызова сотрудника службы безопасности или оповещения этой службы о нападении. Устройство включения сигнализации должно находиться в доступном и скрытом от злоумышленника месте рабочего стола или на полу.

Следовательно, разработка и использование в практической деятельности любой фирмы эффективной системы обеспечения информационной безопасности в процессе приема и работы с посетителями является одной из важных частей системы защиты цен-

ной информации, охраны материальных ценностей фирмы, жизни и здоровья ее персонала.

2.4. Особенности работы с персоналом, владеющим конфиденциальной информацией

2.4.1. Персонал как основная опасность утраты конфиденциальной информации

Если отдельный сотрудник не оправдает доверия, то никакая эффективная система защиты не сможет гарантировать безопасность информации и предотвратить ее разглашение.

В решении проблемы информационной безопасности значительное место занимает выбор эффективных методов работы с персоналом, обладающим конфиденциальной информацией. Персонал генерирует новые идеи, новшества, открытия и изобретения, которые ускоряют научно-технический прогресс, повышают благосостояние сотрудников фирмы и являются полезными не только для фирмы в целом, но и для каждого отдельного сотрудника. Поэтому любой сотрудник объективно заинтересован сохранять в тайне те новшества, которые повышают прибыли и престиж фирмы.

Несмотря на это персонал, к сожалению, является в то же время основным источником утраты ценной и конфиденциальной информации. Объясняется это тем, что с точки зрения психологических особенностей персонал — явление сложное, каждый из сотрудников всегда индивидуален, труднопредсказуем и мотивации его поведения часто противоречивы и не отвечают требованиям сложившейся жизненной ситуации.

Это определяет особую значимость тщательного изучения персонала в структурах, связанных с необходимостью заботиться о сохранении в тайне тех или иных сведений, документов и баз данных. Трудности в работе с персоналом и сложности в подборе достойных во всех отношениях людей испытывает любая фирма, которая использует в работе достаточные объемы конфиденциальных сведений.

В современных предпринимательских структурах практически каждый основной сотрудник становится носителем ценных сведений, которые представляют интерес для конкурентов и криминальных структур. В контексте безопасности кадровая политика имеет профилактическую роль по отношению к такому типу угрозы, как неблагонадежность отдельных сотрудников.

Вопросы управления персоналом, работа которого связана с обработкой, хранением и использованием конфиденциальных сведений, документов и баз данных, в настоящее время все в большей степени в концептуальном и практическом аспектах включаются в число главных при решении проблем информационной безопасности.

Информационная безопасность понимается как защищенность информации на любых носителях от случайных и преднамеренных несанкционированных воздействий естественного и искусственного свойства, направленных на уничтожение, разрушение, видоизменение тех или иных данных, изменение степени доступности ценных сведений.

Помимо профессиональных способностей, сотрудники, связанные с секретами фирмы, должны обладать высокими моральными качествами, порядочностью, исполнительностью и ответственностью.

Они добровольно соглашаются на определенные ограничения в использовании информационных ресурсов и вырабатывают самодисциплину, самоконтроль действий, поступков и высказываний.

Зарубежные специалисты считают, что сохранность конфиденциальной информации на 80% зависит от правильного подбора, расстановки и воспитания персонала фирмы.

Повышение ответственности персонала за выполняемую работу, сохранность ценных сведений, активное участие в принятии управленческих решений требует нового содержания при оценке таких критериев, как образование, профессионализм, личная культура, моральные качества и этика работников. Люди рассматриваются как самый ценный ресурс фирмы и решают, с одной стороны, производственные и коммерческие задачи, а с другой — получают во владение ценные и конфиденциальные

сведения фирмы и обеспечивают их правильное использование и сохранность.

Человеческий фактор должен постоянно учитываться в долговременной стратегии фирмы и ее текущей деятельности, являться основным элементом построения действенной и эффективной системы защиты информационных ресурсов.

Организационные мероприятия по работе с персоналом, получающим доступ к конфиденциальной информации, можно разделить на несколько групп:

1) проведение усложненных аналитических процедур при приеме и увольнении сотрудников;

2) документирование добровольного согласия лица не разглашать конфиденциальные сведения и соблюдать правила обеспечения безопасности информации;

3) инструктирование и обучение сотрудников практическим действиям по защите информации;

4) контроль за выполнением персоналом требований по защите информации, стимулирование ответственного отношения к сохранению конфиденциальных сведений.

Сложности в работе с персоналом определяются:

- большой ценой решения о допуске лица к тайне предприятия;
- наличием в фирме, как правило, небольшого контингента сотрудников, служебные обязанности которых связаны с использованием конфиденциальных сведений (руководители, ответственные исполнители, сотрудники службы конфиденциальной документации);
- разбиением тайны на отдельные элементы, каждый из которых известен определенным сотрудникам в соответствии с направлением их деятельности.

Персонал является основным и самым трудноконтролируемым источником ценной и конфиденциальной информации.

Источник, который называется "персонал и окружающие фирму люди", включает в себя:

- всех сотрудников данной фирмы, ее персонал;
- сотрудников других фирм — посредников, изготовителей комплектующих деталей, торговых фирм, рекламных агентств и т. п.);

• сотрудников государственных учреждений, к которым фирма обращается в соответствии с законом — налоговых и иных инспекций, муниципальных органов, правоохранительных органов и т. д.;

• журналистов средств массовой информации, сотрудничающих с фирмой;

• посетителей фирмы, работников коммунальных служб, почтовых служащих, работников служб экстремальной помощи и т. д.;

• посторонних лиц, работающих или проживающих рядом со зданием или помещениями фирмы, уличных прохожих;

• родственников, знакомых и друзей всех указанных выше лиц.

Перечисленные лица в той или иной мере являются или могут стать в силу обстоятельств источниками конфиденциальных сведений. Каждый из источников, особенно ставший им случайно, может стать опасным для фирмы в результате несанкционированного разглашения (оглашения) защищаемых сведений.

Наиболее осведомлены о секретах фирмы первый руководитель, его основной заместитель, их референты и секретари, работники службы конфиденциальной документации.

Следовательно, персонал фирмы, владеющий ценной и конфиденциальной информацией, работающий с конфиденциальными делами и базами данных, является наиболее осведомленным и часто доступным источником для злоумышленника, желающего получить необходимые ему сведения.

Причем овладение требуемой информацией происходит в значительном числе случает в результате безответственности и необученности персонала, его недостаточно высоких личных и моральных качеств.

2.4.2. Методы добывания ценной информации у персонала

Прежде всего следует выделить так называемое ***осознанное сотрудничество*** работника фирмы со злоумышленником.

К такому сотрудничеству можно отнести:

• инициативное сотрудничество работника фирмы с целью мести руководству или коллективу фирмы, а также по причине подкупа, регулярной оплаты постоянных услуг и психической неустойчивости;

• формирование сообщества — злоумышленник и его сообщник, помощник, работающий на основе убеждения в справедливости взглядов злоумышленника, дружеских и иных отношений, взаимопомощи и т. п.

• сотрудничество на основе личного убеждения работника в противоправных действиях руководства фирмы или их моральном разложении;

• склонение (принуждение, побуждение) к сотрудничеству путем обманных действий, изменения взглядов или моральных принципов путем убеждения вымогательства, шантажа, использования отрицательных черт характера, физического насилия.

Наиболее частым, достаточно опасным и трудновыявляемым является использование сотрудника фирмы для ***неосознанного сотрудничества***:

• переманивание ценных и осведомленных специалистов обещанием лучшего материального вознаграждения, лучших условий труда и иных преимуществ ("кража мозгов");

• ложная инициатива в приеме сотрудника на высокооплачиваемую работу в конкурирующую фирму, выведывание в процессе собеседования необходимых конфиденциальных сведений и затем отказ в приеме;

• выведывание ценной информации у сотрудника фирмы с помощью подготовленной системы вопросов на научных конференциях, встречах с прессой, на выставках, в личных беседах в служебной и неслужебной обстановке;

• подслушивание и записывание на диктофон разговоров сотрудников фирмы в служебных и неслужебных помещениях, в процессе переговоров и приема посетителей, в транспорте, на банкетах, в домашней обстановке, при общении с друзьями и знакомыми;

• прослушивание служебных и личных телефонов сотрудников фирмы, перехват сообщений по электронной почте, вскрытие и ознакомление со служебной и личной корреспонденцией руководства фирмы, сотрудников (иногда при содействии секретаря);

• получение злоумышленником нужной информации от сотрудника под действием алкоголя, наркотиков, психотропных препаратов, внушений, гипноза и т. д.

Ошибочные и безответственные действия персонала обычно подразделяют на две группы:

1) не спровоцированные злоумышленником: взятие конфиденциальных документов на дом; оставление без надзора документа или загруженного компьютера; выбрасывание в мусорную корзину черновиков и копий конфиденциальных документов; использование конфиденциальной информации в открытых публикациях; ошибочная выдача конфиденциального документа сотруднику, не имеющему к нему доступа, и т. п.;

2) спровоцированные злоумышленником: предоставление конфиденциальной информации в ходе ложных социологических и других опросов, ложного анкетирования; допуск злоумышленника или его сообщника в режимное помещение, на территорию фирмы по фиктивным документам; общение сотрудника с легендированным злоумышленником по поводу сведений, составляющих тайну, и т. п.

Результативность обмана зависит от подготовки, интуиции и сообразительности сотрудников, которых провоцируют на ошибочные действия. Сотрудники должны быть обучены и готовы к противодействию подобным действиям злоумышленника или его сообщников, посторонних лиц.

Хорошие деловые отношения обычно складываются у злоумышленника с сотрудниками, которые обижены на руководство фирмы или структурного подразделения, незаслуженно забыты при выдвижении на должность или повышении окладов, не получили материального или морального поощрения за успехи в работе, испортили отношения с коллективом или неформальным лидером коллектива.

Неустойчивый и сложный психологический климат в коллективе фирмы является надежной основой для успешной работы даже не очень опытного злоумышленника и его помощников.

Личные и бытовые затруднения сотрудников, на которые не обращает внимание руководство фирмы, также являются хорошей почвой для работы злоумышленника, например, временные материальные затруднения, жилищные проблемы, тяжелые заболевания близких людей, трудности с детьми, шантаж криминальных элементов и т. п.

Чаще всего злоумышленник выявляет сотрудников, обладающих человеческими слабостями, которые можно развивать и использовать с пользой для его дела, например, болтливость, амбициозность, легкомыслие, стремление к развлечениям, любовь к незаработанным деньгам и другие качества, которые формируют безответственность и ведут к разглашению тайны фирмы.

В этом случае злоумышленник с успехом использует лесть, обещания, подарки, установление дружеских и близких отношений, одалживание денег и т. п. Он играет также на естественном стремлении сотрудника показаться более компетентным, осведомленным и значимым в делах фирмы, особенно если этот сотрудник находился в состоянии алкогольного опьянения или под действием наркотика, психотропного препарата.

Но наиболее частой причиной разглашения секретов фирмы являются обычная глупость сотрудника или его неумение оценивать ситуацию, незнание методов эффективного противодействия злоумышленнику, т. е. плохой подбор персонала и его необученность.

В результате незнания правил защиты информации конфиденциальная информация несанкционированно разглашается на общедоступных научных семинарах, выставках, официальных и неофициальных встречах и презентациях, особенно коллегам по профессии и журналистам.

Очень опасны лица, уволенные из фирмы и владеющие ее конфиденциальной информацией.

Даже поверхностный анализ некоторых способов добывания конфиденциальной информации, которые используют злоумышленники при содействии персонала, показывает, что система защиты секретов фирмы должна прежде всего основываться на тщательном отборе персонала, анализе его личных и моральных качеств, обучении сотрудников правилам защиты информации и противодействия злоумышленникам, создании в фирме здорового психологического климата, воспитании у сотрудников фирменной гордости.

2.4.3. Особенности приема и перевода сотрудников на работу, связанную с владением конфиденциальной информацией

Процессу приема сотрудника на работу предшествует ряд подготовительных этапов, которые позволяют составить точное представление о том, какой специалист и какой квалификации действительно нужен для данной должности, какими деловыми, моральными и личными качествами он должен обладать. Особенно это касается должностей, связанных с владением конфиденциальной информацией.

Можно выделить следующие этапы:

1) предварительно сформулировать, какие функции должен выполнять сотрудник, каков круг его ответственности, какие качества, знания и уровень квалификации необходимо иметь претенденту;

2) составить перечень ценных и конфиденциальных сведений, с которыми будет работать специалист;

3) составить перечень форм поощрения и стимулирования, которые может получать сотрудник;

4) составить другие перечни вопросов, которые необходимо будет решать специалисту, перечни его личных качеств, возрастных, профессиональных и иных характеристик;

5) составить описание должности — документ, аналогичный по структуре должностной инструкции, который определяет требования к кандидату на должность (но это документ — вспомогательный).

Выполнение указанных этапов облегчит процедуру подбора кандидатов и сделает их отбор более обоснованным и объективным. Кандидаты предварительно знакомятся с указанными выше документами, что делает собеседование с ними более целенаправленным и конкретным.

Кроме того, ознакомившись с документами, кандидат может отказаться от предлагаемой работы. Описание вакантной должности имеет для работодателя примерно такое же значение, как и резюме для кандидата.

Поиск кандидата на вновь создаваемую или вакантную должность в фирме не должен носить бессистемный характер. Случайный человек, пришедший с улицы, в определенной степени таит опасность для фирмы как с точки зрения его профессиональной пригодности, так и личных, моральных качеств.

Особую опасность подобный метод подбора представляет для должностей, связанных с владением конфиденциальной информацией или материальными ценностями.

Случайные претенденты на должность обычно рассылают или разносят по предприятиям, учреждениям и фирмам свое резюме. Им не важно, где работать, их просто интересует работа по данной специальности.

С другой стороны, случайный человек не всегда плох и поэтому данный метод при подборе персонала является наиболее распространенным и объективно завоевал право на существование. Но дело в том, что он не должен быть единственным.

Помимо пассивного ожидания прихода нужного человека, существует ряд эффективных направлений активного поиска кандидатов на вакантную должность или рабочее место.

К числу основных направлений можно отнести следующие:

1. Поиск кандидатов внутри фирмы, особенно если речь идет о руководителе или специалисте высокого уровня. Этот метод дает возможность продвигать перспективных работников по служебной лестнице и заинтересовывать их работой, воспитывать преданность делам фирмы. Можно приглашать на должность лицо, ранее работавшее в фирме и хорошо себя зарекомендовавшее.

Перераспределение персонала в соответствии с его склонностями и способностями всегда способствует улучшению работы фирмы и обеспечению ее информационной безопасности. Но надо учитывать, что поддерживается коллективом только такое продвижение по службе, которое определяется высокими деловыми качествами работника. Не может получить одобрения персонала выдвижение плохого работника, в частности, по принципу личных связей или знакомства.

Большим преимуществом этого метода является то, что о кандидате достаточно много известно всему коллективу и судить о профессиональных, моральных и личных качествах, соответствии предлагаемой должности можно на основании достаточно обширного опыта.

Метод имеет недостаток, который состоит в том, что без притока новых людей коллектив теряет свои новаторские качества. Новые люди — это новые идеи, предложения и перспективы развития. Тем не менее этот метод является наилучшим и наиболее надежным при подборе кандидата на должность, связанную с владением ценной и конфиденциальной информацией.

2. Поиск кандидатов среди студентов и выпускников учебных заведений, установление связей с подразделениями вузов, занятыми трудоустройством выпускников. Таким образом можно получить достаточно полную информацию о профессиональных и личных качествах студентов. Очень эффективно вести поиск (даже на средних курсах) наиболее способных студентов, привлекать их в процессе учебы к работе в организации, отплачивать их труд и, может быть, финансировать обучение в вузе, платить стипендию. Коллектив фирмы должен регулярно омолаживаться. Это лекарство от застоя идей, путь к успеху.

3. Обращение в государственные и частные бюро, агентства по найму рабочей силы, биржи труда, организации по трудоустройству лиц, уволенных по сокращению штатов, трудоустройству молодежи, бывших военнослужащих и т. п. Подобные агентства предлагают требуемый контингент работников на имеющиеся рабочие места, ведут целенаправленный поиск не-

обходимого специалиста высокой квалификации, организуют переподготовку специалистов по индивидуальным заказам.

При обращении в агентство необходимо составить перечень служебных обязанностей и требований к нужному работнику, без указания конфиденциальных сведений, с которыми будет связана работа.

4. Рекомендации работающих в фирме сотрудников. Обычно такие рекомендации отличаются ответственным и взвешенным характером, так как с рекомендуемыми людьми сотрудникам придется работать вместе.

Указанные направления поиска кандидатов на должности, связанные с владением конфиденциальной информацией, как правило, позволяют выбрать необходимых работников из ряда лиц, изъявивших желание занять вакантную должность.

Технологическая цепочка приема сотрудников, работа которых связана с владением ценной информацией, включает следующие процедуры:

1) подбор предполагаемого кандидата (кандидатов) для приема на работу или перевода, получение резюме;

2) изучение резюме (и личного дела, если кандидат работает в фирме) руководством фирмы, структурного подразделения и службой персонала, вызов для беседы подходящих кандидатов;

3) информирование кандидатов, работающих в фирме, об их будущих должностных обязанностях, связанных с владением тайной фирмы;

4) знакомство (предварительное собеседование) руководства фирмы, структурного подразделения и службы персонала с кандидатами, не работающими в фирме; беседа с ними, уточнение отдельных положений резюме; ответы на вопросы о будущей работе; изучение полученных от кандидата рекомендательных писем;

5) заполнение кандидатами, не работающими в фирме, и представление в отдел кадров заявления о приеме, автобиографии, личного листка по учету кадров (с цветной фотокарточкой), копий документов об образовании, наличии ученых степеней, ученых и по-

четных званий, передача в отдел кадров рекомендательных писем и характеристик;

6) обновление материалов личного дела работающего в фирме сотрудника; получение представления о переводе на новую должность от руководителя структурного подразделения;

7) собеседование кандидатов с работником отдела кадров по представленным документам, при необходимости подтверждение тех или иных сведений представлением дополнительных документов;

8) опрос сотрудником отдела кадров авторитетных для фирмы лиц, лично знающих кандидата на должность, протоколирование опроса;

9) собеседование экспертов с кандидатами с целью определения их личных и моральных качеств, а для не работающих в фирме сотрудников дополнительно — профессиональных способностей; рассмотрение медицинских справок;

10) при необходимости — тестирование и анкетирование кандидатов;

11) по совокупности собранных материалов и их анализа принятие руководством фирмы решения об отборе единственного претендента и возможности предложить ему работу, связанную с владением тайной фирмы;

12) заключительное собеседование с претендентом на должность, получение от него принципиального согласия на работу с конфиденциальной информацией;

13) в случае согласия — подписание претендентом обязательства о неразглашении тайны фирмы, в частности, сообщаемых ему конфиденциальных сведений; информирование претендента о характере конфиденциальной информации, с которой он будет работать, о наличии системы защиты этой информации и тех ограничениях, которые придется учитывать работнику в служебной и неслужебной обстановке;

14) беседа-инструктаж руководителя структурного подразделения, руководителя службы безопасности и сотрудника службы персонала с претендентом на должность; ознакомле-

ние претендента с должностной инструкцией, рабочими технологическими инструкциями, инструкцией по обеспечению информационной безопасности фирмы и другими аналогичными материалами;

15) составление проекта контракта, содержащего пункт об обязанности работника не разглашать конфиденциальные сведения фирмы;

16) подписание контракта о временной работе без права доступа к конфиденциальной информации;

17) составление и подписание приказа о приеме на работу с испытательным сроком (или на временную работу);

18) заведение личного дела на вновь принятого сотрудника;

19) заполнение на сотрудника необходимых учетных форм, в том числе личной карточки;

20) внесение фамилии сотрудника в первичные учетные бухгалтерские документы;

21) внесение соответствующей записи в трудовую книжку сотрудника;

22) изучение личных, моральных и профессиональных качеств сотрудника в течение испытательного срока;

23) обучение сотрудника правилам работы с конфиденциальной информацией и документами, инструктажи, проверка знаний;

24) анализ результатов работы сотрудника в течение испытательного срока, составление нового контракта о длительной работе и издание соответствующего приказа или отказ сотрудника в работе;

25) оформление допуска сотрудника к конфиденциальной информации и документам.

Предоставленный комплект документов, из которых в дальнейшем будет сформировано личное дело сотрудника, является предметом тщательного изучения руководителями фирмы, структурного подразделения, коллегиального органа управления и службы персонала при решении вопроса о назначении данного лица на должность.

Изучение документов не должно носить формально-бюрократический характер и быть единственным критерием решения вопроса о назначении данного лица на должность.

Изучение документов следует сочетать с объективным анализом нескольких личностей, претендующих на должность, сопоставлением результатов собеседований, тестирования, опросов и т. п. Все это в совокупности позволит на конкурсной или неконкурсной основе правильно провести отбор именно того претендента на должность, который более всего отвечает составленным ранее требованиям.

Предоставленные кандидатом персональные документы тщательно проверяются на достоверность.

При каких-то сомнениях кандидата просят представить дубликаты испорченных документов, заверить исправления. Сведения, включенные в характеристики, рекомендательные письма, списки научных трудов и изобретений, выданные и заверенные другими учреждениями, могут быть проверены путем обращения в эти учреждения.

Документы, явно недостоверные, могут быть возвращены гражданину, и одновременно ему отказывается в рассмотрении вопроса о приеме на работу без объяснения причины отказа.

Сведения, указываемые в резюме, не проверяются.

Заявление о назначении (переводе) на должность, личный листок по учету кадров, автобиография пишутся или заполняются гражданином собственноручно, без использования пишущей машинки или принтера.

Все записи, сделанные в личном листке по учету кадров, и текст автобиографии сравниваются сотрудником отдела кадров с персональными документами. Неподтвержденные записи, на которых настаивает гражданин, дополняются записью сотрудника отдела кадров "со слов гражданина". Исправления в указанных документах не допускаются.

Копии с аттестатов, дипломов, свидетельств, грамот и т. п., которые приобщаются к документам для решения вопроса о приеме на работу, снимаются с помощью копировальной техники в отделе кадров и заверяются сотрудником отдела. Копии,

принесенные гражданином, внимательно сличаются с подлинником и также заверяются этим сотрудником. Нотариального заверения копий не требуется. Запрещается заверение копий с копии.

Паспорт, военный билет, дипломы, аттестаты и другие подобные персональные документы после работы с ними сотрудника отдела кадров возвращаются гражданину (кроме трудовой книжки).

При подборе персонала для работы с ценной или конфиденциальной информацией следует в первую очередь обращать внимание на личные и моральные качества кандидатов на должность, их порядочность и лишь затем — на их профессиональные знания, умения и навыки.

Важно уже на первых этапах отбора исключить те кандидатуры, которые по формальным признакам явно не соответствуют требованиям, предъявляемым к будущему сотруднику.

Собеседование с кандидатами на должность преследует следующие цели:

1) выявить реальную причину желания работать в данной фирме;

2) выявить возможных злоумышленников или попытаться увидеть слабости кандидата как человека, которые могут провоцировать преступные действия;

3) убедиться, что кандидат не намерен использовать в работе секреты фирмы, в которой он раньше работал;

4) убедиться в добровольном согласии кандидата соблюдать правила защиты информации и иметь определенные ограничения в профессиональной и личной жизни.

Вопросники для собеседования составляются таким образом, чтобы выяснить:

- причины увольнения кандидата с прежнего места работы;
- источник информации о вакансии в данной фирме — кто подсказал, кто рекомендовал и т. п.;
- работал ли кандидат ранее с конфиденциальной информацией, подписывал ли обязательство о ее неразглашении;

• отношения в семье, уровень благосостояния кандидата, жилищные условия, культурный уровень и т. п.

Ответы кандидата фиксируются, и те из них, которые вызвали сомнения, уточняются путем опроса знающих кандидата лиц, путем тестирования и другими способами (если это необходимо).

При приеме на работу, связанную с информацией особой предпринимательской важности, для сбора полных сведений о кандидате могут привлекаться работники частных детективных агентств.

Одной из главных задач собеседования и тестирования является выявление несоответствия мотиваций в различных логических группах вопросов. Например, кандидат хочет получать большую зарплату, но раньше он получал столько же; работал близко от дома, а хочет работать в фирме, находящейся на значительном расстоянии, и т. п.

С точки зрения безопасности, ***психологический отбор*** преследует следующие цели:

1) выявление имевших ранее место судимостей, преступных связей, криминальных наклонностей;

2) определение возможных преступных наклонностей, предрасположенности кандидата к совершению противоправных действий, дерзких и необдуманных поступков в случае формирования в его окружении определенных обстоятельств;

3) установление факторов, свидетельствующих о морально-психологической ненадежности, неустойчивости, уязвимости кандидата и т. д.

По мнению многих специалистов-психологов, основные личные качества, которыми должен обладать потенциальный сотрудник, включают:

• порядочность, честность, принципиальность и добросовестность;
• исполнительность, дисциплинированность;
• эмоциональную устойчивость (самообладание);
• стремление к успеху и порядку в работе;
• самоконтроль в поступках и действиях;

• правильную оценку собственных возможностей и способностей;

• умеренную склонность к риску;

• умение хранить секреты;

• тренированное внимание;

• хорошую память, способности к сравнительной оценке фактов и т. д.

Личные качества, не способствующие сохранению секретов:

• эмоциональная неуравновешенность;

• разочарование в себе и своих способностях;

• отчуждение от коллектива;

• недовольство своим служебным положением;

• ущемленное самолюбие;

• крайне эгоистическое поведение;

• отсутствие достаточного благоразумия;

• нежелание и неспособность защищать информацию;

• нечестность;

• финансовая безответственность;

• употребление наркотиков;

• отрицательное воздействие алкоголя, приводящее к болтливости, необдуманным поступкам и т. д.

Не следует думать, что психологический отбор полностью заменяет прежние, достаточно надежные кадровые процедуры (анализ документов, собеседование, опросы сослуживцев и лиц, знающих кандидата, оперативную проверку в правоохранительных органах и т. д.).

Только при умелом сочетании традиционных и психологических кадровых методов анализа можно с определенной степенью достоверности прогнозировать поведение сотрудников в различных, в том числе экстремальных, ситуациях.

Обычно отобранным для работы считается кандидат, у которого результаты анализа документов, собеседований, проверок, тестов и психологического изучения не противоречат друг другу и не содержат данных, которые препятствовали бы приему на работу.

Материалы проверок и анализа кандидатов на должность (в том числе вопросники и протоколы собеседований, заполненные тесты, а также используемые виды тестов и "ключи" к тестам, тестовые нормы, инструкции по проведению и интерпретации и другие подобные материалы) являются строго конфиденциальной информацией.

Обязательство о неразглашении конфиденциальной информации и сохранении тайны фирмы претендент подписывает до того, как ему будет сообщен состав ценных сведений, с которыми ему предстоит работать, и порядок защиты этих сведений.

Обязательство (подписка, соглашение) о неразглашении конфиденциальных сведений представляет собой правовой документ, которым претендент добровольно и письменно дает согласие на ограничение его прав в отношении использования конфиденциальной информации. Одновременно в обязательстве претендент предупреждается об ответственности за разглашение этой информации.

В частности, многие американские фирмы включают в соглашение (обязательство) следующие пункты:

1) детальное изложение принципов определения конкретных сведений, составляющих тайну фирмы;

2) краткое изложение порядка охраны конфиденциальных сведений;

3) меры, которые должен принимать сам работник для обеспечения сохранности этих сведений;

4) перечень административных наказаний, которым может быть подвергнут работник, разгласивший сведения, составляющие тайну фирмы (увольнение, понижение в должности, перевод на другую работу и т. п.).

Хорошо, если обязательство содержит пункт о том, что сотрудник не будет использовать в своей деятельности информацию, принадлежащую на правах собственности фирме, в которой он ранее работал.

Подобные обязательства подписывают не только претенденты на работу в данной фирме, но и все лица, тем или иным образом

участвующие в работе фирмы и потенциально имеющие возможность узнать элементы тайны фирмы (например, акционеры, поставщики, сотрудники работающих с фирмой рекламных и торговых структур, эксперты и т. п.).

Подписание обязательства о неразглашении тайны фирмы следует предусмотреть для служащих фирмы, которые не имеют непосредственного отношения к закрытым сведениям, однако могут ознакомиться с ними при исполнении служебных обязанностей (шоферы, дворники, уборщицы, сотрудники охраны и др.).

Считается, что обязательство о неразглашении тайны фирмы не дает полной гарантии сохранения этих сведений, однако, как показывает практика, существенно снижает риск их разглашения персоналом или иными лицами, риск незаконного их использования, а также число попыток конкурентов внедрить в фирму свою агентуру.

После подписания обязательства и проведения беседы-инструктажа с претендентом заключается трудовой договор (контракт).

В контракте должен быть пункт об обязанности работника не разглашать сведения, составляющие тайну фирмы, а также конфиденциальные сведения партнеров и клиентов, об обязательстве соблюдать правила защиты конфиденциальных сведений. Может быть пункт о собственности фирмы на результаты работы сотрудника, на сделанные им изобретения и открытия и согласии сотрудника на публикацию этих достижений только с разрешения руководства фирмы.

Часто в контракте содержится пункт об обязанности сотрудника сообщать в службу безопасности обо всех попытках посторонних лиц получить у него конфиденциальную информацию. В обязательном порядке включается пункт об обязанности сотрудника немедленно сообщать непосредственному руководителю и службе безопасности об утере носителей конфиденциальной информации, документов, дел, конфиденциальных материалов, изделий и т. п.

В заключительной части указывается степень ответственности за разглашение тайны фирмы или несоблюдение правил защи-

ты информации. Обычно это расторжение трудового договора, при необходимости — последующее судебное разбирательство.

Отличием индивидуальных трудовых соглашений от трудовых договоров (контрактов) в части сохранения коммерческой тайны является то, что в трудовых соглашениях должны быть указаны конкретные сведения, составляющие предпринимательскую тайну фирмы и доверенные сотруднику в связи с выполнением им работы, а также конкретные меры по обеспечению сохранности этих сведений.

После подписания приказа о приеме на работу в отделе кадров формируется личное дело сотрудника, включающее стандартный набор документов.

Материалы, связанные с профессиональным и психологическим анализом данного работника (протоколы собеседований, тесты, протоколы бесед и опросов и т. п.), подшиваются в дело кадровой службы "Материалы по приему сотрудников на работу", но не в личное дело сотрудника. Дело с материалами имеет гриф конфиденциальности "Строго конфиденциально".

Вести какие-либо досье на сотрудников, содержащие сведения, полученные неофициальным путем, запрещается.

После получения допуска к конфиденциальной информации сотрудник в индивидуальном порядке должен быть обучен правилам работы с документами, базами данных, которые будут ему предоставлены. Результат обучения фиксируется в обязательстве или контракте. Отметка заверяется подписями руководителя службы безопасности и сотрудника.

Усложненные процедуры приема на работу, связанную с владением конфиденциальной информацией, и проверки достоверности сведений, указанных в документах, позволяют всесторонне оценить кандидата на должность. С другой стороны, они дают возможность руководству фирмы и самому кандидату оценить ситуацию и без спешки принять правильное решение.

Методы психологического анализа, проводимые одновременно с хорошо зарекомендовавшими себя приемами анализа доку-

ментов претендента на должность, позволяют сделать достаточно обоснованные выводы о пригодности данного лица для замещения вакантной должности, связанной с владением конфиденциальной информацией. Следует учитывать, что использование только психологических методов анализа личности не дает достоверного результата и может иметь лишь рекомендательный характер.

2.4.4. Доступ персонала к конфиденциальным сведениям, документам и базам данных

Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных является одной из центральных проблем системы защиты информации. Регламентация порядка доступа лежит в основе режима конфиденциальности проводимых фирмой работ. Важно четко и однозначно определить: кто, кого, к каким сведениям, когда и как допускает.

Режим представляет собой совокупность ограничительных правил, мероприятий, норм, обеспечивающих контролируемый доступ на определенную территорию, в помещения, к информации и документам. Любой режим базируется на так называемой разрешительной системе.

Разрешительная система в общем виде предусматривает необходимость получения специального разрешения на осуществление соответствующих правовых мероприятий, например, на въезд в пограничную зону, на посещение воинской части и т. п.

Разрешительная (разграничительная) система доступа в сфере коммерческой тайны представляет собой совокупность правовых норм и требований, устанавливаемых первым руководителем или коллективным органом руководства фирмой с целью обеспечения правомерного ознакомления и использования сотрудниками фирмы конфиденциальных сведений, необходимых им для выполнения служебных обязанностей.

Принципы построения разрешительной системы доступа:

• надежность, т. е. относительное исключение возможности несанкционированного доступа посторонних лиц к документам в обычных и экстремальных условиях;

• полнота охвата всех категорий исполнителей и всех категорий документов, информации на любых носителях;

• конкретность, т. е. исключение двоякого толкования и однозначность решения о доступе;

• производственная необходимость как единственный критерий доступа исполнителя к документу, а также доступа к документам представителей государственных служб;

• определенность состава и компетенции должностных лиц, дающих разрешение на доступ исполнителя к конфиденциальным сведениям, документам и базам данных, исключение возможности бесконтрольной и несанкционированной выдачи таких разрешений;

• строгая регламентация порядка работы всех категорий сотрудников фирмы с информацией, документами и базами данных.

Разрешительная система решает задачи:

— ограничения и регламентации состава сотрудников, функциональные обязанности которых требуют знания тайны фирмы и работы с ценными документами;

— строгого избирательного и обоснованного распределения документов и информации между сотрудниками;

— обеспечения сотрудника всем необходимым для реализации своих служебных функций (документами, делами, базами данных, информацией, техническими средствами и т. д.);

— беспрепятственного прохода сотрудника в здание фирмы, в конкретное рабочее помещение (режимную зону), к выделенному ему офисному рабочему оборудованию и компьютеру;

— исключения для посторонних лиц возможности несанкционированного ознакомления с конфиденциальной информацией;

— рационального размещения рабочих мест сотрудников, при котором исключалось бы бесконтрольное использование сотрудником защищаемой информации.

Разрешительная система включает в себя две составные части: допуск сотрудника к конфиденциальной информации и непосредственный доступ этого сотрудника к конкретным сведениям.

Под ***допуском*** понимается процедура оформления права сотрудника фирмы или иного лица на доступ к сведениям (информации) ограниченного распространения и одновременно — правовой акт согласия (разрешения) собственника (владельца) информации на передачу ее для работы конкретному лицу.

Оформление допуска, т. е. согласия лица на определенные ограничения в использовании информации, всегда носит добровольный характер. Наличие допуска предоставляет сотруднику формальное право работать со строго определенным кругом конфиденциальных документов, баз данных и отдельных сведений.

Как отмечалось выше, к конфиденциальной информации допускаются, как правило, лица, проработавшие в фирме определенное время и зарекомендовавшие себя с положительной стороны.

В предпринимательских структурах разрешение на допуск дает первый руководитель фирмы. Разрешение оформляется соответствующим пунктом в контракте (трудовом договоре).

Допуск может оформляться приказом первого руководителя с указанием типового состава сведений, с которыми разрешается работать данному сотруднику или группе сотрудников.

Допуск может носить временный характер (на период выполнения определенной работы) и пересматриваться при изменении профиля работы сотрудника.

Законодательством США предусмотрено, что никто не имеет права иметь допуск к засекреченной информации лишь благодаря своему чину или положению. Конечной инстанцией, решающей вопрос о необходимости допуска данному лицу, является руководитель, который распоряжается этой информацией и осуществляет за ней контроль.

Доступ — практическая реализация каждым сотрудником предоставленного ему допуском права на ознакомление и работу с определенным составом конфиденциальных сведений, документов и баз данных. Он санкционируется полномочным должностным лицом (первым руководителем, его заместителем, руководителем подразделения, службы или направления деятельности) в отношении

конкретной информации и конкретного сотрудника. Право на выдачу такого разрешения строго регламентируется.

Разрешение (санкция) на доступ к конкретной информации может быть дано при соблюдении следующих условий:

- наличие подписанного приказа первого руководителя о приеме на работу (переводе, временном замещении, изменении должностных обязанностей и т. п.) или назначении на должность, в функциональную структуру которой входит работа с данной, конкретной информацией;
- наличие подписанного сторонами трудового договора (контракта), имеющего пункт о сохранении тайны фирмы, и подписанного обязательства о неразглашении ставших известными конфиденциальных сведений и соблюдении правил их защиты;
- соответствие функциональных обязанностей сотрудника передаваемым ему документам и информации;
- знание сотрудником требований нормативно-методических документов по защите информации и сохранению тайны фирмы;
- наличие в офисе необходимых условий для работы с конфиденциальными документами и базами данных;
- наличие систем контроля за работой сотрудника.

Особенность информационного обслуживания потребителей конфиденциальной информации заключается в том, что вопросы определения состава необходимой им информации решаются полномочным руководителем, а не самими потребителями.

Существует общее, обязательное правило: исполнители, которым документ не адресован руководителем, не только не имеют права доступа к нему, но и не должны знать о существовании такого документа и исходных данных о нем.

Структура процедуры разграничения доступа должна быть многоуровневой, иерархической. Иерархическая последовательность доступа к информации реализуется по принципу "чем выше уровень доступа, тем уже круг допущенных лиц; чем выше ценность сведений, тем меньшее число сотрудников может их знать".

В фирме может составляться схема выдачи разрешений на доступ к массовой конфиденциальной информации. Такая схема разрабатывается с учетом двух аспектов: выдачи разрешений в зависимости от категорий документов и выдачи разрешений в зависимости от занимаемой должности. Графы схемы: категории документов; должностные лица, дающие разрешение; категории исполнителей, которым дается разрешение.

В схеме отражаются также категории документов, с которыми определенные категории исполнителей знакомятся без специального разрешения.

Может составляться матрица полномочий, в которой по горизонтали стоят наименования категорий документов, по вертикали — фамилии или должности сотрудников.

Всю конфиденциальную информацию фирмы может знать только первый руководитель фирмы.

Конфиденциальную информацию по конкретной работе в полном объеме вправе получать лишь соответствующий заместитель первого руководителя, руководители структурных подразделений или направлений деятельности по специальному перечню, утвержденному первым руководителем.

Необходимо добиваться минимизации привилегий персонала по доступу к информации. При сбое в системе защиты информации или обнаружении факта утраты информации должно мгновенно вводиться ограничение или прекращение доступа к любой конфиденциальной информации до окончания служебного расследования.

Разграничение доступа основывается на однозначном расчленении информации по тематическим группам, уровням конфиденциальности этих групп и пользователям, которым эта информация необходима для работы. Задачей процедуры разграничения доступа является регламентация минимальных потребностей персонала в конфиденциальных сведениях.

Это дает возможность разделить знание элементов коммерческой тайны среди как можно большего числа сотрудников. Например, желательно, чтобы целиком идею, формулу, конструкцию не знал никто, каждый знал бы лишь свою незначительную часть.

Дробление информации также не позволяет конкурентам использовать ее за счет прима на работу уволенного из фирмы сотрудника.

При составлении конфиденциального документа следует учитывать, что его содержание не только определяет его функциональное назначение, но и лежит в основе разрешительной процедуры доступа персонала к данному документу.

Поэтому документ необходимо посвящать только одной тематической группе вопросов, предназначенной, по возможности, одному конкретному исполнителю или структурному подразделению.

В соответствии с иерархической последовательностью доступа определяется структура рубежей защиты информации, которая предусматривает постепенное ужесточение защитных мер с ростом уровня конфиденциальности сведений. Этим обеспечивается недоступность этих сведений для случайных людей, злоумышленника и определяется необходимый уровень защищенности информации.

Разрешение на доступ к конфиденциальным сведениям строго персонифицировано, т. е. руководители несут персональную ответственность за правильность выдаваемых ими разрешений на доступ исполнителей к конфиденциальным сведениям, а лица, работающие с конфиденциальными документами, несут персональную ответственность за сохранение в тайне их содержания, сохранность носителя и соблюдение установленных правил работы с документами.

Руководитель фирмы имеет право давать разрешение на ознакомление со всеми видами конфиденциальных документов фирмы и всем категориям исполнителей и другим лицам. Однако целесообразно, чтобы первый руководитель оставлял за собой право распоряжаться только наиболее ценной информацией, делегируя право выдачи разрешений на доступ к другой информации нижестоящим руководителям.

Следует иметь в виду, что чрезмерная централизация выдачи разрешений на доступ к конфиденциальной информации неизбежно ведет к снижению оперативности в решении произ-

водственных вопросов. Излишняя децентрализация и либерализация создают условия для утраты ценных сведений.

Заместители первого руководителя по функциональным сферам (по науке, производственным вопросам, сбыту и др.) имеют право давать разрешение на ознакомление с конфиденциальными сведениями всем нижестоящим руководителям и исполнителям, но в пределах своей компетенции.

Руководителям структурных подразделений дается право разрешать доступ к конфиденциальным сведения всем работникам своих подразделений по тематике их работы. Руководитель подразделения может давать разрешение только непосредственно подчиненным ему сотрудникам. Для осуществления доступа к документам данного подразделения работника другого подразделения необходимо разрешение соответствующего заместителя руководителя фирмы.

Ответственные исполнители работ (направлений деятельности) имею право давать разрешение на доступ к конфиденциальной информации подчиненным им исполнителям и в пределах их компетенции.

В небольших фирмах разрешение на доступ дает только первый руководитель.

Представителям государственных органов разрешение на доступ к конфиденциальным сведениям дает только первый руководитель фирмы.

При необходимости доступа к конфиденциальным сведения представителей других фирм и предприятий руководствуются теми обязательствами, которые были закреплены в соответствующем договоре (контракте) на выполнение работ или услуг.

Это касается как документированной информации, так и устной, визуальной и любой другой. В этом случае разрешение на доступ дает должностное лицо фирмы, включенное в специальный перечень, прилагаемый к договору и утвержденный первым руководителем.

Разрешение на доступ к конфиденциальным сведениям представителя другой фирмы или предприятия оформляется резолюцией

полномочного должностного лица на предписании (или письме, обязательстве), представленном заинтересованным лицом.

В резолюции должны быть указаны конкретные документы или сведения, к которым разрешен доступ. Одновременно указывается фамилия сотрудника фирмы, который знакомит представителя другого предприятия с этими сведениями и несет ответственность за его работу в помещении фирмы.

Руководитель фирмы, вне зависимости от формы ее собственности, может устанавливать иные специальные или дополнительные правила доступа к конфиденциальным сведениям, документам, базам данных и носителям информации, конфиденциальным изделиям и продукции фирмы. Он несет за это единоличную ответственность.

Разрешение на доступ к конфиденциальной информации всегда дается полномочным руководителем только в письменном виде: резолюцией на документе; приказом, утверждающим схему именного или должностного доступа к конкретным группам информации; утвержденным руководителем списком-разрешением на обложке дела; списком ознакомления с документом и т. п.

Без дополнительного разрешения допускаются к документам их исполнители (если они продолжают работать по той же тематике) и лица, визировавшие, подписавшие, утвердившие документ. Без специального разрешения могут допускаться также лица, указанные в тексте распорядительных документов.

Если сотрудник допускается только к части документа, то в разрешении (резолюции) четко указываются конкретные пункты, разделы, страницы, приложения, с которыми он может ознакомиться. Сотрудник службы конфиденциальной документации (КД) обязан принять необходимые меры по исключению возможности ознакомления исполнителя с другими частями документа.

Следует соблюдать правило, по которому регистрируются все лица, имеющие доступ к определенным документам, коммерческим секретам. Это позволяет на высоком уровне осуществлять информационное обеспечение аналитической работы по выявлению возможных каналов утраты информации.

При организации доступа сотрудников фирмы к конфиденциальным массивам электронных документов, базам данных необходимо помнить о его многоступенчатом характере.

1. *Доступ к персональному компьютеру, серверу или рабочей станции* предусматривает:

• определение и регламентацию первым руководителем фирмы состава сотрудников, имеющих право доступа (входа) в помещение, в котором находится соответствующая вычислительная техника, средства связи;

• регламентацию первым руководителем временного режима нахождения этих лиц в указанных помещениях;

• организацию охраны этих помещений в рабочее и нерабочее время, определение правил вскрытия помещений и отключения охранных технических средств информации и сигнализирования;

• определение правил постановки помещений на охрану;

• регламентацию работы указанных технических средств в рабочее время;

• организацию контролируемого (в необходимых случаях — пропускного) режима входа в указанные помещения и выхода из них;

• организацию действий охраны и персонала в экстремальных ситуациях или при авариях техники и оборудования помещений;

• организацию выноса из указанных помещений материальных ценностей, машинных и бумажных носителей информации; контроль вносимых в помещение и выносимых персоналом личных вещей.

Несмотря на то что по окончании рабочего дня конфиденциальные сведения должны быть перенесены на гибкие носители и стерты с жесткого диска компьютера, помещения, в которых находится вычислительная техника, подлежат охране.

Объясняется это тем, что, во-первых, в неохраняемый компьютер легко установить какое-либо средство промышленного шпионажа, во-вторых, злоумышленник может с помощью специальных методов восстановить стертую конфиденциальную информацию на жестком диске (произвести "уборку мусора").

2. *Доступ к машинным носителям конфиденциальной информации, хранящимся вне ПК* предполагает:

• организацию учета и выдачи сотрудникам чистых машинных носителей информации;

• организацию ежедневной фиксируемой выдачи сотрудникам и приема от сотрудников носителей с записанной информацией (основных и резервных);

• определение и регламентацию первым руководителем состава сотрудников, имеющих право оперировать конфиденциальной информацией с помощью компьютеров, установленных на их рабочих местах, и получать учтенные машинные носители информации;

• организацию системы закрепления за сотрудниками машинных носителей информации и контроля за сохранностью и целостностью информации, учета динамики изменения состава записанной информации;

• организацию порядка уничтожения информации на носителе, порядка и условий физического уничтожения носителя;

• организацию хранения машинных носителей в службе конфиденциальной документации в рабочее и нерабочее время, регламентацию порядка эвакуации носителей в экстремальных ситуациях;

• определение и регламентацию первым руководителем состава сотрудников, не сдающих по объективным причинам технические носители информации на хранение в службу КД в конце рабочего дня, организацию особой охраны помещений и компьютеров этих сотрудников.

Работа сотрудников службы КД и фирмы в целом с машинными носителями информации вне ПК должна быть организована аналогично работе с бумажными конфиденциальными документами.

3. *Доступ к конфиденциальным базам данных и файлам* является завершающим этапом доступа сотрудника фирмы к компьютеру. И если этот сотрудник — злоумышленник, то можно считать, что самые серьезные рубежи защиты охраняемой электрон-

ной информации он успешно прошел. В конечном счете он может просто унести компьютер или вынуть из него и унести жесткий диск, не "взламывая" базу данных.

Обычно доступ к базам данных и файлам подразумевает:

• определение и регламентацию первым руководителем состава сотрудников, допускаемых к работе с определенными базами данных и файлами;

• именование баз данных и файлов, фиксирование в машинной памяти имен пользователей и операторов, имеющих право доступа к ним;

• учет состава базы данных и файлов, регулярную проверку наличия, целостности и комплектности электронных документов;

• регистрацию входа в базу данных, автоматическую регистрацию имени пользователя и времени работы;

• сохранение первоначальной информации;

• регистрацию попытки несанкционированного входа в базу данных, регистрацию ошибочных действий пользователя, автоматическую передачу сигнала тревоги охране и автоматическое отключение компьютера;

• установление и нерегулярное по сроку изменение имен пользователей, массивов и файлов (паролей, кодов, классификаторов, ключевых слов и т. п.), особенно при частой смене персонала;

• отключение компьютера при нарушениях в системе регулирования доступа или сбое системы защиты информации;

• механическое (ключом или иным приспособлением) блокирование отключенного, но загруженного компьютера при недлительных перерывах в работе пользователя.

Коды, пароли, ключевые слова, ключи, шифры, специальные программные продукты, аппаратные средства и другие атрибуты системы защиты информации в ПК разрабатываются, меняются специализированной организацией и индивидуально доводятся до сведения каждого пользователя работником этой организации или системным администратором. Применение пользователем собственных кодов не допускается.

Процедуры допуска и доступа сотрудников к конфиденциальной информации завершают процесс включения данного сотрудника в состав лиц, реально владеющих тайной фирмы. С этого времени большое значение приобретает текущая работа с персоналом, в распоряжении которого находятся ценные и конфиденциальные сведения.

2.4.5. Текущая работа с персоналом, владеющим конфиденциальной информацией

По мнению большинства специалистов по безопасности информационных систем, главное внимание должно быть обращено на персонал, постоянно работающий с конфиденциальными документами и базами данных.

Текущая работа с персоналом, обладающим конфиденциальной информацией, включает в себя:

- обучение и систематическое инструктирование сотрудников;
- проведение регулярной воспитательной работы с персоналом, работающим с конфиденциальными сведениями и документами;
- постоянный контроль за выполнением персоналом требований по защите конфиденциальной информации;
- изучение степени осведомленности персонала в области конфиденциальных работ фирмы;
- проведение служебных расследований по фактам утечки информации и нарушений персоналом требований по защите информации;
- совершенствование методики текущей работы с персоналом.

Процесс обучения сотрудников фирмы правилам защиты информации должен быть постоянным, так как система защиты требует регулярного обновления и видоизменения. Занятия не должны превращаться в редкие, необязательные и формальные собрания.

Обучение сотрудника начинается с момента проведения собеседования при приеме на работу и подписания им обязательства о неразглашении тайны и заканчивается в момент увольнения и подписания этим лицом обязательства о недопустимости использования конфиденциальных сведений в чьих-либо целях.

Обучение сотрудников может начинаться также с момента начала работы коллектива над новой идеей, оцененной в качестве фирменного секрета, работы с использованием ноу-хау и т. п.

Обычная периодичность обучения для работающих сотрудников — один раз в 3–5 лет, как правило, после аттестации или перезаключения контракта.

Задачи обучения включают в себя изучение следующих вопросов:

- характера и состава конфиденциальной информации;
- возможных угроз конфиденциальным сведениям, каналов их объективного распространения и каналов утраты, методов работы злоумышленников;
- структуры системы защиты, требований и правил защиты конфиденциальной информации;
- порядка работы сотрудников с конфиденциальными сведениями, документами и базами данных;
- действий персонала в конкретных экстремальных ситуациях.

Обучение сотрудников предполагает приобретение и поддержание на высоком уровне производственных навыков работы с конфиденциальными сведениями, воспитание глубокой убежденности в необходимости выполнения требований по защите любой конфиденциальной информации.

Персонал должен получить знания по оценке важности тех или иных сведений для упрочения престижа фирмы и ее финансовой стабильности, а значит, и для благополучия каждого сотрудника.

Методика обучения сотрудников включает в себя:

- специализированные программы обучения для обеспечения лекционных курсов и практических занятий;

• проведение лекций, семинаров и собеседований как общеознакомительного плана, так и по конкретным направлениям защиты; тестирование сотрудников;

• решение ситуационных задач, связанных с выполнением необходимых требований по защите конфиденциальной информации;

• практическую ситуационную учебу по действиям персонала в экстремальных ситуациях;

• проведение деловых игр, обучающих методам противодействия замыслам злоумышленника.

Очень важно сделать процесс обучения индивидуализированным. Он должен быть конкретизирован по должностному составу сотрудников, по типовым рабочим местам и часто — по отдельным сотрудникам.

В процессе обучения сотрудник должен получить только те знания, которые ему необходимы для работы. Избыточности знаний в области состава конфиденциальной информации и способов ее защиты не должно быть.

Отдельно от остального персонала обучаются сотрудники службы безопасности, секретарь, сотрудники, работающие с особо ценными документами, делами и изделиями.

Информация, сообщаемая в процессе обучения сотрудников, является строго конфиденциальной. Конспекты, записи сотрудники делают в специальных тетрадях, хранящихся в соответствии с общим порядком работы с конфиденциальными документами.

По окончании обучения проводится проверка усвоения сотрудниками полученных знаний. Результаты проверки фиксируются в протоколе комиссии, ведущей проверку.

Целесообразно организовывать проверку знаний путем тестирования или решения ситуационной задачи. Сотрудники, не прошедшие проверку знаний, от работы с конфиденциальной информацией отстраняются.

Одновременно с обучением должны проводиться регулярные ***совещания-инструктажи*** с сотрудниками. В процессе инструктажа:

• до сведения сотрудников доводятся изменения и дополнения, внесенные в действующие нормативно-методические до-

кументы по защите информации, приказы и указания руководства фирмы в области защиты информации и информационной безопасности;

• сотрудники информируются о конкретных угрозах информации, каналах утечки информации, действиях злоумышленников, принятых дополнительных мерах по защите информации;

• анализируются случаи нарушения сотрудниками правил защиты информации, сообщается о фактах утраты секретов по вине сотрудников.

Инструктаж, так же как и обучение, проводится индивидуально, информация, сообщаемая на инструктажах, разглашению не подлежит. Совещания-инструктажи проводятся, как правило, по мере необходимости.

Обязательной и первостепенной частью текущей работы с персоналом должно стать обучение сотрудников правилам работы с конфиденциальной информацией, документами и базами данных. Трудно говорить об эффективности работы с персоналом, если сотрудники не имеют достаточно твердых представлений о системе защиты конфиденциальной информации, методах противодействия злоумышленникам.

Обучение и инструктаж находятся в тесной связи с ***процессом воспитания сотрудников***, направленным на то, чтобы привить им устойчивые мотивационные стереотипы поведения в ситуации, связанной с обеспечением недоступности информации посторонним лицам, исключением возможности несанкционированного доступа этих лиц к ценным и конфиденциальным сведениям.

Текущая или профилактическая работа с персоналом является обязательной составной частью предотвращения попыток отдельных сотрудников воспользоваться в личных целях ценной для фирмы информацией, нарушить требования обеспечения информационной безопасности фирмы.

Каждый из сотрудников фирмы, работающий с закрытыми сведениями, документами и базами данных, должен находиться под

постоянным наблюдением руководства и коллектива фирмы, оценивающих степень его лояльности по отношению к делам фирмы.

Со своей стороны фирма обязана обеспечить любому сотруднику необходимые условия труда и отдыха, постоянно заботиться о его благополучии, повышении квалификации и поддержании на высоком уровне интереса к выполняемым обязанностям и работам.

Между руководством и сотрудниками не может быть глухой стены непонимания стоящих задач. Все дела фирмы должны быть важны для коллектива в целом и для каждого отдельного сотрудника.

Достигается это сложным и длительным процессом индивидуального воспитания сотрудников на основах взаимного доверия, взаимопонимания и заботы. Руководители всех рангов несут персональную ответственность за качество этой работы.

В основе воспитательной работы с персоналом фирмы должны лежать не пустые словесные увещевания о необходимости хорошо работать и грядущем благополучии для всего персонала.

Дальновидные руководители серьезных фирм под воспитательной работой подразумевают прежде всего создание реально здорового психологического климата в коллективе фирмы, позволяющего объединить осознанные усилия персонала для решения стоящих перед фирмой задач и преодоления возникающих трудностей.

Здоровый психологический климат в коллективе фирмы создает труднопреодолимый барьер на пути любого злоумышленника, который пытается получить конфиденциальные сведения.

Для сотрудника фирмы часто важен не столько оклад, который он получает, сколько та доброжелательная обстановка, которая существует в коллективе, уверенность в том, что его уважают как специалиста, ценят его упорный труд и он может надеяться на продвижение по службе.

При хорошем психологическом климате сотрудники доброжелательно относятся к любым ограничениям, связанным с функци-

онированием системы защиты информации, добровольно, с пониманием важности выполняют все требования этой системы.

Здоровый психологический климат должен включать в себя следующие основные элементы:

• постоянное изучение и анализ комплекса качеств каждого сотрудника фирмы, т. е. знание каждого сотрудника в отдельности, а не абстрактная воспитательная работа с коллективом;

• строгое выполнение пунктов и положений коллективного договора;

• создание реальных условий для продвижения сотрудников по службе или повышение оклада с учетом их трудовых достижений, а не по иным причинам;

• оплата фирмой обучения или переподготовки способных и ценных для фирмы сотрудников;

• строгое выполнение администрацией норм техники безопасности и охраны труда, создание наилучших условий для работы сотрудников и их отдыха;

• своевременное выявление неформальных лидеров в коллективе, выдвижение их на руководящие должности или перевод в другие подразделения (при их отрицательном влиянии на коллектив — увольнение);

• участие администрации фирмы в решении личных и бытовых затруднений сотрудников;

• охрана сотрудников, гарантия юридической и физической защиты в случае попыток криминальных действий злоумышленника по отношению к ним, их родственникам и близким людям.

Процесс обучения и воспитания сотрудников фирмы должен завершаться ***контролем работы персонала с конфиденциальной информацией и документами***. Важен контроль защиты ценной информации от недобросовестных посягательств отдельных сотрудников.

Превентивный контроль работы персонала предполагает прежде всего наличие в фирме строгого учета степени осведомленности каждого сотрудника о фирменных секретах.

В данном случае учет создает информационную базу не только для облегчения контрольной функции, но и для аналитических исследований по обнаружению каналов утраты защищаемой информации.

Следует соблюдать правило, по которому в обычном принудительном режиме регистрируются все лица, имеющие доступ к определенным документам, базам данных и носителям коммерческих секретов.

Одновременно подлежат специальному (экстремальному) учету все замеченные несанкционированные или ошибочные действия персонала с документами и информацией, нарушения системы доступа к информации и правил работы с конфиденциальными документами и базами электронных данных. Подобные факты подлежат оперативному, тщательному сравнительному анализу, а результаты анализа должны докладываться непосредственно первому руководителю фирмы.

Регулярный и своевременный учет состава конфиденциальной информации, известной каждому из сотрудников фирмы, является наиболее информативной частью контрольной работы. Учитываются любые контакты любого сотрудника с конфиденциальными сведениями, в том числе санкционированные, а также случайное, несанкционированное ознакомление с информацией, к которой сотрудник не имеет доступа, в том числе несанкционированное ознакомление с конфиденциальной информацией сотрудников, вообще не имеющих доступа к подобной информации.

Традиционная (карточная) или электронная учетная форма должна содержать ряд предметных зон, позволяющих сопоставлять функциональные обязанности сотрудника и состав конфиденциальной информации.

Целесообразно включить в учетную форму следующие зоны:

• зону штатных функциональных обязанностей сотрудника, при реализации которых используется конфиденциальная информация (по утвержденной должностной инструкции);

• зону изменений и дополнений, внесенных в функциональные обязанности сотрудника, с указанием документа-ос-

нования, его даты и фамилии руководителя, подписавшего документ;

• зону стандартного состава конфиденциальных сведений и их индексов (по перечню конфиденциальной информации), к которым допущен сотрудник в соответствии с должностной инструкцией (с указанием наименования документа о допуске, его даты, номера и фамилии руководителя, подписавшего документ);

• зону изменений и дополнений в составе конфиденциальных сведений и их индексов по перечню, к которым допускается сотрудник в связи с пересмотром его должностных обязанностей (с указанием наименований и дат документов о допуске, фамилий руководителей, подписавших документы);

• зону документированной информации (документов), с которой знакомится или работает сотрудник, с указанием наименований документов, их дат и номеров, краткого содержания, целевого использования содержащихся в документах конфиденциальных сведений и их индексов по перечню, фамилий руководителей, разрешивших работу с документами;

• зону недокументированной конфиденциальной информации, которая стала известна сотруднику, с указанием даты и цели ознакомления, фамилии руководителя, разрешившего ознакомление, состава конфиденциальных сведений и их индексов по перечню;

• зону обнаруженного несанкционированного ознакомления сотрудника с конфиденциальной информацией с указанием даты, условий или причин ознакомления, фамилии виновного сотрудника, места ознакомления, состава конфиденциальных сведений и их индексов по перечню.

Анализ осуществляется сравнением содержания записей в зонах и индексов известной сотруднику конфиденциальной информации, т. е. ведется поиск несоответствия.

Работник, ответственно относящийся к своей работе и участвующий в делах и прибылях фирмы, как правило, так же ответственно относится к сохранению конфиденциальности тех работ, которые ведет фирма, строго соблюдает требования информационной безопасности и защиты информации.

Основными формами контроля качества работы персонала, профессиональных знаний, в том числе в части защиты информации, являются:

- аттестация сотрудников;
- отчеты руководителей подразделений о работе подразделений и состоянии системы защиты информации;
- регулярные проверки руководителем фирмы или службой безопасности соблюдения сотрудниками требований по защите информации;
- самоконтроль сотрудников.

Аттестация сотрудников представляется одной из наиболее эффективных форм контроля их деятельности как в профессиональной сфере, так и в сфере соблюдения информационной безопасности фирмы.

Аттестация персонала — это коллективная форма оценки профессиональной пригодности сотрудника, его соответствия занимаемой должности. Аттестация проводится периодически (ежеквартально, раз в год и в иные сроки).

При проведении аттестации рассматриваются следующие характеристики сотрудника: трудовая дисциплина, исполнительность, трудолюбие, ответственность, требовательность и принципиальность, организованность в работе, качество и эффективность выполняемой работы, самостоятельность и инициатива, творческая деятельность, прогрессивность профессиональных решений, профессиональный кругозор, умение общаться с людьми, организаторские способности, преданность делу фирмы.

В части соблюдения сотрудником требований защиты информации рассматриваются такие характеристики, как знание нормативных и инструктивных документов по защите информации, умение применять требования этих документов в практической деятельности, отсутствие нарушений в работе с конфиденциальными документами, умение общаться с посторонними лицами, не раскрывая секреты фирмы, и т. д. На основе изучения этих характеристик формируется представление о каждом сотруднике, его деловых и человеческих качествах.

По результатам аттестации издается приказ (распоряжение), в котором отражаются решения аттестационной комиссии о поощрении, переаттестации, повышении в должности или увольнении сотрудников. Аттестационная комиссия может также выносить решение об отстранении сотрудника от работы с информацией и документами, составляющими тайну фирмы.

Одна из форм контроля — заслушивание *на совещании у первого руководителя фирмы отчетов руководителей структурных подразделений и руководителя службы безопасности о состоянии системы защиты информации и выполнении ее требований сотрудниками подразделений.* Одновременно на совещании принимаются решения по фактам нарушения сотрудниками этой системы.

Формой контроля являются также *регулярные проверки выполнения сотрудниками* (в том числе хорошо работающими) *правил работы с конфиденциальной информацией, документами и базами данных.* Проверки проводятся руководителями структурных подразделений и направлений деятельности фирмы, заместителями первого руководителя, работниками службы безопасности.

Одновременно с соблюдением сотрудником правил работы с конфиденциальными документами проверяется наличие у этого сотрудника числящихся за ним документов, носителей информации, дел, магнитных, носителей информации, электронных массивов информации, изделий и иных элементов, составляющих тайну фирмы.

Проверки могут быть плановыми и внеплановыми (внезапными). Внезапные проверки проводятся при возникновении малейшего подозрения о разглашении или утечке информации.

Самоконтроль сотрудников фирмы состоит в проверке самими руководителями и исполнителями полноты и правильности выполнения ими действующих инструктивных положений, а также в немедленном информировании непосредственного руководителя и службы безопасности о фактах утери документов, утрате по какой-либо причине ценной информации, разглашении лично или други-

ми сотрудниками сведений, составляющих тайну фирмы, нарушении сотрудниками порядка защиты информации.

При работе с персоналом фирмы следует сосредоточивать внимание не только на сотрудниках, работающих с конфиденциальной информацией. Под контролем должны находиться также лица, не имеющие доступа к тайне фирмы. Можно предполагать, что эти сотрудники могут быть посредниками в действиях злоумышленника: в проведении электронного шпионажа, создании условий для хищения документов, снятии с них копий и т. п.

Кроме того, нужно учитывать, что сотрудники фирмы, работающие с конфиденциальной информацией, вынуждены действовать в рамках требований, регламентированных инструкцией по обеспечению режима конфиденциальности.

Ограничение свободы человека может приводить к стрессам, нервным срывам. Сохранение чего-то в тайне противоречит потребности человека в общении путем обмена информацией. В связи с этим психологический настрой коллектива и отдельных сотрудников всегда должен находиться в центре внимания руководства фирмы.

При невыполнении сотрудниками требований по защите информации к ним должны в обязательном порядке и своевременно применяться меры порицания и наказания в соответствии с правилами внутреннего трудового распорядка: объявление выговора, понижение в должности, лишение премии, отстранение от работы с конфиденциальной информацией, увольнение.

Важно, чтобы наказание было неотвратимым и своевременным, невзирая на должностной уровень сотрудника.

Следует учитывать, что ответственность за разглашение сведений, составляющих тайну фирмы, в первую очередь несут руководители фирмы и ее структурных подразделений, направлений деятельности, филиалов, так как они полностью отвечают за разработку и реализацию мер, обеспечивающих информационную безопасность всех видов деятельности фирмы.

Факт утраты информации выявляется в основном посредством анализа публикаций, рекламы, выставочных и других материалов

фирм-конкурентов. В этом случае анализируются карточки учета осведомленности сотрудников о тайне фирмы и выявляется круг сотрудников, владеющих утраченной информацией. Анализ ведется в рамках служебного расследования.

Служебное расследование организуется по фактам разглашения или утечки информации, утраты документов и изделий, другим грубым нарушениям правил защиты информации.

Расследование проводится специальной комиссией, формируемой приказом первого руководителя фирмы.

Расследование предназначено для выяснения причин, всех обстоятельств и их последствий, связанных с конкретным фактом, установления круга виновных лиц, размера причиненного фирме ущерба. Все мероприятия обязательно документируются.

План проведения служебного расследования:

- определение возможных версий случившегося (утрата, хищение, уничтожение по неосторожности, умышленная передача сведений, неосторожное разглашение и т. д.);
- определение (планирование) конкретных мероприятий по проверке версий (осмотр помещений, полистная проверка документации, опрос сотрудников, взятие письменного объяснения у подозреваемого лица и т. д.);
- назначение лиц, ответственных за проведение каждого мероприятия;
- указание сроков проведения каждого мероприятия;
- определение порядка документирования;
- обобщение и анализ выполненных действий по всем мероприятиям;
- установление причин утраты информации, виновных лиц, объема ущерба для фирмы;
- передача материалов служебного расследования с заключительными выводами первому руководителю фирмы для принятия решения.

Служебное расследование проводится в кратчайшие сроки.

В ходе служебного расследования обычно анализируются следующие виды документов:

- письменные объяснения опрашиваемых лиц, составляемые в произвольной форме;

• акты проверки документации и помещений, где указываются фамилии лиц, проводивших проверку, их должности, объем и виды проведенного осмотра, результаты, подписи этих лиц и дата;

• другие документы, относящиеся к расследованию (справки, заявления, планы и т. д.).

По результатам анализа составляется заключение о результатах проведенного служебного расследования, в котором подробно описывается проведенная работа, указываются причины и условия случившегося, определяются виновные лица, даются рекомендации по предотвращению подобных фактов.

Вопрос о наказании виновных лиц ставится только после завершения служебного расследования, мера наказания определяется лично первым руководителем фирмы.

При подтверждении факта передачи сотрудником информации постороннему лицу фирма должна обратиться в суд для вынесения решения о возмещении материального ущерба от кражи информации.

Рекомендуемые направления и методы текущей работы с персоналом фирмы позволяют организовать эффективную систему заинтересованного участия сотрудников в обеспечении безопасности фирменных секретов, постоянного контроля за работой персонала с конфиденциальной информацией и своевременного выявления попыток злоумышленника завладеть интеллектуальной собственностью фирмы.

2.4.6. Особенности увольнения сотрудников, владеющих конфиденциальной информацией

Стабильность кадрового состава является важнейшей предпосылкой надежной информационной безопасности фирмы. Миграция специалистов — самый трудноконтролируемый канал утраты ценной и конфиденциальной информации. Вместе с тем, полностью избежать увольнений сотрудников не представляется возможным.

Необходим тщательный анализ причин увольнения, на основе которого составляется и реализуется программа, исключающая эти причины.

Например, предусматриваются повышение окладов, аренда жилья для сотрудников вблизи фирмы, оздоровление психологического климата, увольнение руководителей, злоупотребляющих своим служебным положением и др.

Технологическая цепочка увольнения сотрудника включает в себя:

• написание сотрудником заявления об увольнении с подробным раскрытием причины увольнения и желательно — с указанием места предполагаемой работы;

• передачу заявления руководителю структурного подразделения для оформления и передачи в отдел кадров или службу персонала;

• прием службой КД от увольняющегося сотрудника всех числящихся за ним документов, баз данных, носителей информации, изделий, материалов, с которыми он работал, проверка их комплектности, полноты и оформление приема в описи исполнителя или актом;

• сдачу сотрудником пропуска (идентификатора) для входа в рабочую зону, всех ключей и печатей, запрещение сотруднику входить в рабочее помещение с использованием знания шифра кодового замка (при необходимости — изменение кода);

• проведение сотрудником службы безопасности или службы персонала беседы с сотрудником об обязательстве сохранения в тайне тех сведений, которые ему были доверены по службе в фирме, предупреждение сотрудника о запрещении использования этих сведений в интересах конкурента или в личных целях, выяснение причины увольнения и места новой работы;

• подписание сотрудником обязательства о неразглашении им конфиденциальных сведений после увольнения;

• документальное оформление увольнения в соответствии с общими правилами;

• прием от сотрудника пропуска для входа в здание фирмы, выдачу ему трудовой книжки и расчета по заработной плате, сопровождение его до выхода из здания сотрудником службы безопасности.

После сдачи всех документов и материалов сотруднику запрещается входить в режимную рабочую зону. При необхо-

димости у него может быть изъят пропуск (идентификатор) сотрудника и выдан идентификатор посетителя с правом входа только в определенные административные помещения.

Увольняющемуся сотруднику напоминают, что и после увольнения из фирмы по крайней мере в течение года за его деятельностью будет осуществляться наблюдение. Предупреждение включается в обязательство, которое подписывает увольняющийся сотрудник.

В практике США аналогичный порядок рекомендуется применять в отношении консультантов, экспертов и временно работавших сотрудников. По крайней мере, от них целесообразно в обязательном порядке потребовать письменное обязательство о неразглашении ставших известными им фактов и сведений, запрещении использования их в своей деятельности или работе конкурирующих фирм в течение определенного времени.

Эффективным средством против разглашения фирменных секретов в США считается заключение соглашения о предоставлении увольняющимся сотрудником консультационных услуг фирме в течение ряда лет.

В течение этого времени, т. е. срока конфиденциальности известных ему сведений, ему выплачивается жалованье, близкое по размерам к заработной плате. В результате бывший сотрудник противостоит соблазну использовать тайну фирмы в своих интересах.

Ущерб от увольнения сотрудника резко уменьшается, если тайна фирмы раздроблена и известна по частям достаточно большому числу служащих. В этом случае не приходится прибегать к указанным выше сложным и часто малоэффективным способам защиты тайны, известной уволенным сотрудникам.

В любом случае рекомендуется по истечении трех месяцев после увольнения направить бывшему сотруднику письмо-напоминание о необходимости сохранения тайны фирмы.

Если руководству фирмы стали известны случаи несанкционированного использования бывшим сотрудником конфиденциальных сведений или ноу-хау фирмы, следует начать судебное разбирательство.

Рассмотренная технология оформления увольнения сотрудников, владеющих ценными и конфиденциальными сведениями, позволит не только повысить ответственность всего персонала за сохранность доверенных ему сведений, но и предотвратить факты кражи увольняющимися сотрудниками ценной информации, ограничить возможность использования ее в других организациях и фирмах.

3. ЛИЧНАЯ БЕЗОПАСНОСТЬ

3.1. Азбука выживания бизнесмена

Кроме организации безопасности предпринимателя и его фирмы с использованием технической и физической охраны, существует еще один способ — это информационная безопасность.

Носителем информации являются не только жилище, автомобиль, офис, но и одежда и экипировка предпринимателя. Модная яркая одежда предпринимателя привлекает к себе внимание не только девушек и молодых женщин, но и преступников.

Судя по одежде, осанке, поведению человека, можно определить его статус в обществе, материальную обеспеченность, характер и прочее. Очень часто люди, привлекающие к себе внимание, становятся жертвой насилия.

Феномен жертвы изучает наука — виктимология. Она различает два типа людей, обладающих повышенной виктимностью, или индивидуальной предрасположенностью стать жертвой преступления.

Психологи выделяют среди людей *истероидный тип* — человек, которому необходимо привлекать внимание (особенно это характерно для женщин). Его приметы: вызывающая одежда, чересчур громкий разговор или смех в общественном месте (транспорте), пристальный взгляд на окружающих и т. п.

Немецкий психолог Вера Биркенбиль в своей книге "Как добиться успеха в жизни" отмечает: во-первых, существует "язык тела" (выражение лица, звук голоса, жесты); во-вторых, есть дополнительный феномен — человек является тем, что он

о себе думает. Нет необходимости говорить о своем внутреннем состоянии, окружающие почувствуют его и так.

Люди всегда чувствуют, как мы настроены по отношению к ним. На уровне подсознания мы действуем как передатчик, который сообщает окружающим, какое у нас настроение: радостное или печальное, ощущаем ли мы себя победителями или наше чувство самооценки опустилось ниже нулевого.

Умение обеспечить скрытность такой информации о себе — это целое искусство, которым владеют немногие.

Групповая предрасположенность, как правило, связана с профессией человека. Чем больше он привлекает внимание окружающих, тем выше его индекс риска.

Чаще других становятся жертвами преступлений в силу своей профессиональной деятельности, социальной роли, которую они выполняют в обществе, кассиры, инкассаторы, работники полиции, службы безопасности фирм, сторожа и некоторые другие люди, вынужденные в силу служебного долга вступать в конфликт с теми, кто посягает на чужое имущество, жизнь и здоровье граждан, нарушает общественный порядок и нормы общежития.

Криминальная виктимология занимается изучением причин и условий совершения преступлений с позиций поведения жертвы, ее роли в противоправном деянии, а также выработкой научно обоснованных практических рекомендаций для потенциальных жертв, определением для них соответствующих мер безопасности.

Эта научная дисциплина изучает не все преступления, а лишь те из них, в которых противоправные действия вызваны личными качествами либо поведением самого потерпевшего.

Анализ сегодняшних "наработок" криминальной виктимологии позволяет сделать вывод о том, что наиболее часто в роли потерпевших от преступлений оказываются молодежь, старики и, конечно, умственно неполноценные люди.

Наряду с этим, среди жертв преступлений можно выделить определенную категорию лиц с особенностями психологической структуры личности. К их числу относятся люди алчные, с обострен-

ным чувством зависти, пережившие тяжелые эмоциональные потрясения, не уверенные в себе.

Повышенной способностью стать в определенных условиях потерпевшим от преступления наделены также люди, ведущие легкомысленный образ жизни, склонные к авантюризму, злоупотребляющие спиртными напитками, легкомысленно относящиеся к сохранности собственного имущества. Сюда же можно отнести лиц, которые не соблюдают элементарных мер предосторожности в конкретных жизненных ситуациях. Это может вызываться самыми различными причинами: беспечностью, самонадеянностью, заблуждением и, разумеется, влиянием алкоголя.

Наряду с попытками дать общую классификацию жертв правонарушений, криминальная виктимология выделяет также определенные типы потерпевших от конкретных видов преступлений.

Подмечено, к примеру, что жертвами мошенничества зачастую становятся не наивные простаки, а люди нечестные, алчные, стремящиеся получить те или иные, пусть даже мелкие, выгоды, не считаясь с требованиями морали, рассчитывающие удовлетворить свои желания вопреки порядку, даже в ущерб другим гражданам или государству. Такие "ловкачи" чаще других попадают на удочку более ловких мошенников.

Имеющиеся в настоящее время материалы виктимологических исследований приводят к выводу, что большинство жертв воров отличаются беспечностью, легкомыслием, беззаботностью и излишней доверчивостью. Жертвы телесных повреждений отличаются вспыльчивостью, вздорностью, себялюбием, невыдержанностью и чувством превосходства над окружающими.

Преступники, как правило, отлично знают психологию своих потенциальных жертв, используя их "слабости" в своих целях. Брачный аферист выбирает свою жертву среди женщин, не скрывающих страстного желания выйти замуж; карточный шулер — среди жадных до наживы людей; шантажист ищет тех, кому есть что скрывать от других.

Предпринимателю при встрече с уголовником рассчитывать на счастье не следует. Даже мелких бизнесменов — "челноков" — и то видно за версту. Вот почему так важно знать, как достигается информационная безопасность и организуется информационная защита.

Очень часто (особенно в последние годы) в сложных и порой самых неожиданных положениях предпринимателю приходится рассчитывать в первую очередь на самого себя.

Цель данной главы — помочь бизнесмену (предпринимателю) овладеть азами выживания, чтобы быстро ориентироваться и правильно действовать в криминальных ситуациях. Иногда это может стать единственным шансом, который нужно уметь использовать для сохранения своей и чужой жизни.

3.1.1. Защита от злонамеренных действий сотрудников фирмы

Многие бизнесмены и предприниматели, имеющие опыт управления государственным производством, более "уютно" чувствуют себя в "новом качестве", в то время как начинающие деловые люди сталкиваются с массой неизвестных ранее проблем: во-первых, как подобрать "команду" преданных работников, внутри которой преобладают корпоративные отношения, во-вторых, как строить отношения с подчиненными, в-третьих, каким будет отношение сотрудников к владельцу фирмы и его собственности, в-четвертых, как избежать злонамеренных действий сотрудников.

Все эти проблемы взаимосвязаны и взаимозависимы. Принятия одних только организационных и технических мер недостаточно для того, чтобы бизнесмен (предприниматель) обезопасил себя от внутрифирменных конфликтов и различного рода потерь. Важно, чтобы в фирме был благоприятный социально-психологический климат, был стимул к честному труду.

Вполне очевидно, что при проверке и подборе кадров следует особое внимание уделять материальному (имущественному) положению кандидатов на вакантные должности, связанные с матери-

альной и финансовой ответственностью, наличию у них рекомендаций. Желательно также использование различных тестов.

Немаловажно и личное знакомство предпринимателя с потенциальным сотрудником фирмы, чтобы самому составить представление о нем, тех или иных его наклонностях. Правильно поступают те руководители, которые при личной встрече с кандидатом предоставляют возможность побеседовать с ним руководителям ведущих отделов, которые впоследствии доводят свои оценки до предпринимателя.

Не стоит особо доверять первому впечатлению — внешность обманчива. Не следует также переоценивать такие качества, как обходительность и умение произвести благоприятное впечатление. Бизнесмен должен исходить из того, что нынешний безработный уже прочитал не одну популярную брошюру о "технологии карьеры" ("Как составить хорошее профессиональное резюме"; "Как вести себя при встрече с работодателем" и т. п.).

Огромная эрудиция, внешние данные и обаяние — все может говорить в пользу кандидата, и, тем не менее, он (она) может оказаться строптивым, неуравновешенным, склочным, нечестным человеком, не исключено также, что вскроется его принадлежность к "группе повышенного риска" (алкоголик, наркоман, с уголовным прошлым и проч.).

Подобная ошибка может дорого стоить предпринимателю и обернуться "обкрадыванием" фирмы на протяжении длительного периода.

Полезно, чтобы предприниматель усвоил следующее правило: "Как бы остро вы ни нуждались в кадрах, не стоит упрощать процедуру проверки при найме на работу. Помните, что, поступаясь жесткими требованиями при отборе, вы подвергаете риску свои доходы".

Бизнесмен обязан удостовериться в честности каждого вновь принятого на работу служащего, проверив его рекомендации, уточнить мнение руководителей с предыдущего места работы. Среди прочего, это самая надежная мера предосторожности.

Чтобы предприниматель и впрямь чувствовал себя защищенным, он должен знать, как поведут себя подчиненные в той или иной ситуации.

Как поступит, например, сотрудник фирмы, если случайно обнаружит кем-то забытый кошелек или 100-долларовую банкноту? Что он будет делать, если будет отгружено больше продукции, чем указано в накладной? Вернет ли служащий, отвечающий за эту операцию, лишний товар на склад? Попытается ли он присвоить его (возможно, находясь в сговоре с водителем грузовика) или же вовсе ничего не заметит и отправит товар? Как поступит бухгалтер при исчезновении какого-либо счета или платежного документа? Поймет ли, что это означает потерю части прибыли, и обратит ли на это внимание предпринимателя? Возможны и другие варианты.

Отсюда вытекает второе правило: "Доверяя, проверяйте". Проверки сотрудников должны носить незакономерный характер, а также проводиться негласно.

Не меньшим злом являются конфликтные ситуации, которые могут иметь место между предпринимателем и одним из ведущих сотрудников или целой группой сотрудников.

Как правило, конфликт возникает по причине неисполнения обещаний предпринимателем, или когда отдельные сотрудники считают, что их недооценили, занизили оценку их личного вклада, занизили премиальные, гонорар и проч.

Чтобы этого не произошло, предприниматель должен учиться слушать сотрудников. Быть хорошим слушателем — не такое простое искусство. Понимая подтекст и намеки в ходе беседы, совещания или собрания, предприниматель сможет лучше и быстрее локализовать назревающий конфликт, своевременно извиниться за личный просчет или разъяснить обидевшемуся сотруднику причину того или иного решения.

Другое дело, если конфликт достиг апогея. В таких случаях следует выработать правильную тактику. Прежде всего следует помнить об информационной безопасности.

Планы и намерения предпринимателя не должны быть известны склочнику, который не упустит свой шанс: воспользоваться полученной информацией в своих интересах или в интересах других лиц, чтобы подорвать авторитет руководителя, веру в его честность и порядочность, по возможности нанести максимальный урон

фирме. Предприниматель должен всегда соблюдать информационную безопасность и требовать этого от своей команды.

Следует разобраться в неформальной структуре коллектива фирмы. Часто неформальные связи и влияние, неформальное лидерство определяют жизнь организации. Необходимо выявить "узлы" напряженности, ее причину, инициаторов склок или других злонамеренных действий.

План по локализации конфликта составляется с учетом мнения авторитетных сотрудников фирмы.

Поручения по реализации намеченного плана доводятся до каждого исполнителя отдельно, чтобы никто не имел общего представления о его содержании и целях. Эти меры необходимы для исключения утечки информации.

Правильно поступают те предприниматели, которые в трудовом контракте предусматривают увольнение лиц, допустивших не только нарушение трудовой дисциплины, но и нарушение "кодекса чести сотрудника фирмы".

3.1.2. Телефонный шантаж и угрозы в адрес бизнесмена

Для определенного контингента злоумышленников и преступников телефон стал средством извлечения выгоды, шантажа, запугивания, прямого террора. Здесь все зависит от цели, которая ими преследуется.

От того, кому звонит случайный хулиган, он ждет испуга, возмущения, ярости. В этом случае не следует давать звонящему эмоциональной пищи — следует прервать разговор и положить трубку рядом с аппаратом или выдернуть шнур из розетки.

Если у предпринимателя есть основание думать, что надоедать могут десятки людей (такое нередко случается с известными людьми), то по его просьбе за определенную плату городская телефонная сеть может изменить номер телефона и исключить его из картотеки справочно-информационной службы.

Другое дело, если телефон используется для запугивания, вымогательства, угроз. Для предупреждения телефонных звонков любого

из названных вариантов предпринимателю следует заранее запастись соответствующими техническими средствами.

Для этого требуются устройства записи телефонных разговоров для компьютера или мобильного телефона. При этом необходимо проверить, не выдаст ли себя такое устройство разными не характерными для обычных аппаратов звуковыми эффектами. Это может насторожить вымогателя.

Желательно, чтобы включалось записывающее устройство одновременно со снятием телефонной трубки.

В случае его отсутствия можно воспользоваться автоответчиком: если события будут развиваться по нарастающей, полиции пригодятся любые материалы.

Если во время телефонной беседы начинаются угрозы захватить предпринимателя или членов его семьи, следует выяснить, кто истинный хозяин вымогателей и кто из коллег предпринимателя или знакомых мог быть наводчиком. Степень информированности злоумышленника поможет его отыскать, поэтому предприниматель должен спокойно отвечать звонящему, затягивая разговор и получая максимум сведений.

Если позволяет обстановка, кто-нибудь из членов семьи может воспользоваться телефоном соседей, чтобы позвонить на телефонный узел или в службу "102", с тем, чтобы определить, откуда раздался звонок с угрозами.

Если злоумышленник бросил трубку, то не следует нажимать на рычаг, а необходимо положить свою трубку рядом с телефоном — канал связи будет сохраняться больше часа.

В ходе беседы необходимо задавать вымогателям наводящие вопросы, предлагать свои условия сделки, которые могут поставить их в тупик и заставить обратиться к хозяину за консультациями. Во время этой паузы предприниматель сможет определить свою дальнейшую тактику.

Обязательно нужно вспомнить, каким был характер звонка — не был ли он междугородным. Имеет значение начало разговора: первые слова собеседника, представился ли он, уточнил ли, с кем говорит, или сразу начал угрожать.

Предприниматель должен помнить: никогда сразу не следует отказывать вымогателям в их требовании, главное для него — выиграть время. Поэтому здесь уместны разговоры о форме оплаты, переводе наличности, можно попросить номер счета или адрес, по которому доставить деньги, и т. д.

Необходимо убедить злоумышленника в том, что ему готовы заплатить требуемую сумму, но для этого потребуется определенное время, — чтобы продать дачу, машину, снять со счета и т. п.

Если события, которым начали шантажировать предпринимателя, не было, не нужно спешить сообщать об этом собеседнику. Необходимо выяснить как можно больше деталей, требовать новых доказательств и гарантий.

При этом следует вести разговор спокойно, обдумывая каждое слово. Злоумышленник не должен догадаться об испуге или серьезных переживаниях. Рекомендуется сделать два глубоких вдоха и выдоха, чтобы восстановить дыхание, растянуть рот в улыбке, представив этот разговор как "детскую игру", хотя и не самую удачную.

Необходимо первое время строить простые фразы, допускать небольшие паузы, пока не восстановится нормальное состояние, и предприниматель почувствует уверенность, тем более, что пока ничего серьезного не произошло.

Очень важно для предпринимателя обратить внимание на следующие детали разговора:

1) быстро или медленно произносились слова, внятно или нет;

2) не слышно ли было каких-либо дефектов речи, заикания, акцента или других особенностей;

3) каков тембр голоса, громким или тихим он был, не было ли в нем хрипоты, сопения, покашливания. Не показалось ли, что говорящий нетрезв или болен;

4) что характерного в манере говорить: спокойная ли речь и уверенная или невнятная и бессвязная; вежливая или грубая; эмоциональная или бесцветная; не почувствовалась ли озлобленность или подчеркнутое равнодушие;

5) не слышно ли было посторонних шумов, сопровождающих разговор; другого голоса, подсказывающего что-то собеседнику; многоголосого шума или шума станков, машин, телефонных разговоров, объявлений по радио; транспорта (поезда, уличного шума, гула метро).

Правильно поступит предприниматель (даже в случае, когда разговор записан на диктофон), если все свои первые впечатления запишет в блокнот или на лист бумаги. Не следует надеяться на свою память, в экстремальной ситуации и в волнении она часто подводит.

В любом случае, подвергаясь телефонному террору, необходимо сохранять присутствие духа. Это поможет сориентироваться в сложившейся ситуации и найти решение, наилучшее для данного случая.

В системе личной безопасности всегда важны первые шаги: экстремальную ситуацию можно обойти или оборвать в самом начале. Этому помогут основные правила информационной безопасности, которые должны стать частью бытовой культуры предпринимателя и членов его семьи.

Например, не называть своего имени или телефонного номера. Пользуясь автоответчиком, не следует указывать номер телефона или имя, нельзя сообщать, что никого нет дома. Текст для автоответчика следует составить таким образом, чтобы из него было понятно только то, что хозяин занят и сейчас не может снять трубку.

В случае телефонного звонка с угрозами непосредственно предпринимателю не рекомендуется сразу же звонить в милицию, службу безопасности или друзьям, так как телефон может находиться под контролем.

Вначале необходимо оценить обстановку: кто мог быть наводчиком; кто знал об упоминаемых событиях; нет ли знакомых, сослуживцев с подобной манерой разговора или тембром голоса; кто знал номер телефона (если это прежде держалось в секрете) и прочее.

Диктофонную запись нужно дать послушать знакомым и соседям — может быть, кто-то узнает говорящего, или какая-либо, на

первый взгляд, незначительная деталь подскажет нужное направление поиска.

Необходимо реально оценить возможности и шансы правоохранительных органов, так как подчас в городских управлениях не хватает элементарной техники, людей для организации наружного наблюдения, личной охраны.

Если предприниматель решил работать с полицией, а не с частным сыскным агентством, то необходимо обязательно написать заявление на имя начальника отделения полиции и передать его оперативному дежурному, который выдаст в ответ талон-уведомление. При этом он должен сообщить номер телефона, по которому надо будет позвонить при следующем разговоре с злоумышленником.

Лучше всего вышеизложенное проводить с помощью верного человека, так как возле полиции может быть установлено наблюдение.

Перед передачей магнитофонной записи следователю предприниматель должен сделать несколько копий записи и спрятать их у верных людей, которые в случае необходимости помогут восстановить справедливость.

Никакие искажения не помогут злоумышленнику замаскировать голос. Специалисты фоноэкспертизы могут даже дать примерные сведения о возрасте человека, уровне его образования, некоторых чертах характера, месте рождения.

Такая методика действий при шантаже и угрозах по телефону поможет предпринимателю предотвратить захват в заложники родных и близких, а также сохранить свое материальное положение.

3.1.3. Захват в заложники предпринимателя (ведущего специалиста), членов его семьи. Киднеппинг

Главный капитал любой фирмы — люди. Именно от них зависит ее процветание. Но не от каждого — в равной степени, так как все сотрудники выполняют не одни и те же роли на производстве.

Например, ведущих специалистов фирмы оберегают не только на территории, но и вне ее, а в некоторых случаях и дома, зачастую круглосуточно. Безопасность специалиста может быть неудобна для него, так как одновременно предполагает охрану членов семьи и других родственников, их жилья, имущества, машин.

Причем эти меры не всегда означают, что за предпринимателем ходит тенью телохранитель. К его услугам средства личной безопасности, разрабатываемые специализированными фирмами: бронежилеты, радиомаяки, радиопередатчики, шифрозамки, сейфы, транспортные средства, детекторы взрывчатых веществ, сигнальные средства и др.

В последние годы, когда рэкет из разряда экстраординарных явлений перешел в разряд обыденных, участились и "непопулярные" ранее случаи похищения людей с целью выкупа.

При расследовании преступлений, связанных с захватом заложников, была выявлена закономерность: все они осуществлялись с помощью наводок.

Практически всем случаям захвата заложников с целью выкупа предшествуют переговоры между преступниками и будущей жертвой, наедине или по телефону. То ли русская беспечность, то ли недооценка противника очень часто не приводят к положительным — для предпринимателя — результатам.

Поэтому, если предприниматель, конечно, в состоянии предвидеть такой ход событий, необходимо оборудовать свой кабинет скрытыми техническими средствами записи.

Тактика поведения во время предварительных переговоров по телефону аналогична описанной в предыдущем разделе.

В России каждый гражданин может быть похищенным. Рожденное в 1930-х гг. понятие "киднеппинг" обязано своим происхождением гангстерам Чикаго, которые воровали детей богатых родителей ради получения выкупа.

Сегодня действует несколько десятков группировок, специализирующихся на похищении различных категорий населения:

1. ***Похищение младенцев***. Цель — продажа детей за границу в бездетные семьи. Отдельно стоят похищения детей цыгана-

ми. Тогда украденный ребенок используется цыганками-побирушками.

2. ***Похищение детей и подростков.*** Практикуется повсеместно, используется различными преступными группировками как метод воздействия на конкурентов и бизнесменов. Цель — либо "чистое" взимание денег, либо склонение родителей похищенного к сотрудничеству. Судьба похищенного ребенка может сложиться по-разному.

Вероятность возврата его родителям довольно велика, если родители вносят выкуп как можно скорее после похищения.

Если же ребенок похищен не с целью вымогательства, а с целью личной мести, его могут убить, уже получив выкуп.

Такое происходит, если у преступников имеется уверенность, что родители предпримут ответные шаги. Оставленный в живых ребенок в таком случае может оказаться ненужным свидетелем, запомнившим место содержания, сообщников похитителей, дорогу, по которой его везли.

Вносить выкуп следует так, чтобы преступники доставляли в условленное место живого ребенка. Нельзя отдавать деньги, поддавшись обещаниям, что через определенное время он вернется домой.

3. ***Похищение молодых девушек*** для поставки "белых рабынь" в публичные дома Южной Азии и Ближнего Востока.

4. ***Похищение неимущих.*** Производится преступными группировками, практикующими вымогательство у крупных бизнесменов или склонение последних к сотрудничеству. Обычно жертвами таких преступников становятся бомжи, не имеющие родственников. Похищенного бомжа на глазах у точно так же похищенного бизнесмена пытают или убивают, причем весьма жестокими способами, обещая очевидцу: *"Не будешь слушаться, с тобой поступят так же".*

5. ***Похищение стариков.*** В настоящее время стало редким, но не искоренено окончательно. Целью может быть завладение жилой площадью.

Ребенок с раннего детства должен быть приучен к тому, чтобы не вступать в общение с незнакомыми людьми, если он находится без сопровождающего.

Полиция многих стран считает обязательным для любого ребенка закон четырех "НЕ":

1) не разговаривай с незнакомцем;

2) не садись в машину к незнакомцу;

3) не играй по дороге из школы домой;

4) не оставайся на улице с наступлением темноты.

Предлог, которым воспользуется злоумышленник, предсказать невозможно. Ребенок должен твердо усвоить, что если он один, то на любое приглашение, предложение незнакомого человека следует сказать: *"Извините, нет"* и отойти.

Очень важно объяснить, что незнакомый — это всякий, кого не знает сам ребенок. Незнакомец может назвать его по имени, сказать, что пришел по просьбе мамы. Но если человек ребенку незнаком, контакт с ним недопустим.

Если тот оказывается слишком навязчивым или пытается увести куда-то ребенка силой, нужно кричать: *"Я его не знаю!"* Родителям необходимо внушить ребенку, что никогда, ни при каких обстоятельствах они не пришлют за ним в школу, домой или во двор незнакомого ему человека.

Если такой человек подойдет, кем бы он ни назвался, надо немедленно бежать в людное место, позвонить родителям или обратиться к полицейскому.

В круг незнакомцев для ребенка должны быть включены и сверстники, и те, кто младше. Не только потому, что порой именно они заманивают жертву в машину к взрослым злоумышленникам, но из-за "детского рэкета", драк и т. д.

Мальчику надо внушить, что на таком его качестве, как смелость, кто-то может сыграть, поэтому осмотрительность и осторожность вовсе не противоречат храбрости, а любая вещь или предмет, которые у него хотят отнять, стоит меньше его здоровья и безопасности.

Часто не только отсутствие находчивости, но и хорошее воспитание мешает детям действовать решительно в минуту опасности. Ребенку следует иметь представление о том, что и воспитанный человек должен уметь постоять за себя.

Если ребенок еще мал, родители должны сказать ему, что не будут сердиться, если он начнет грубить, громко кричать, отбиваться, кусаться, когда к нему станет приставать незнакомый человек. Следует объяснить ребенку взрослое понятие "право на собственную оборону".

Любой ребенок, начиная с 3-летнего возраста, и тем более школьник, должен знать:

1) свои имя, фамилию, отчество, возраст;

2) домашний адрес, домашний телефон;

3) имена и фамилии родителей, места их работы и телефоны;

4) место своей учебы (школу, класс);

5) возможные маршруты движения по району.

Каждый ребенок должен знать круг людей, к которым по их профессиональной принадлежности можно обращаться за помощью: работники полиции, метро, продавцы магазинов, служащие учреждений.

Не стоит игнорировать мировую практику идентификации детей. Способы различны. Это может быть жетон с личными данными, адресом и телефоном; визитка, готовая метка на одежде с указанием данных и проч.

Дети постарше могут иметь средства личной безопасности (звуковые сирены, которые хороши для привлечения внимания окружающих и при защите от животных; средства радиоконтроля в заданной зоне; газовые аэрозольные упаковки); естественно, что необходимы дисциплина, ответственность и навыки в обращении.

Если у ребенка свой ключ от квартиры, никогда не вешайте его ему на шею. Приучите его к тому, чтобы он не забывал его в дверях, в почтовом ящике, в кармане пальто. Лучший вариант — оставить ключ у кого-то из соседей, потому что здесь появляется дополнительный контроль.

Оставшись один в квартире, ребенок должен знать, что дверь всегда нужно закрывать не только на замок, но и на задвижку или цепочку.

Ребенку необходимо твердо усвоить, что нельзя вступать в переговоры с кем-то незнакомым через дверь. В ответ на просьбу открыть, дать стакан воды, помочь соседу или маме, на уверения, что цель визита — проверка работы электричества, газа, крана, ребенку следует сказать: *"Сейчас я позвоню соседу, он выйдет и поможет вам"* или: *"Я позвоню в полицию, они приедут и все решат"*.

Ребенок должен понимать также, что и он ни под каким предлогом не может выходить из квартиры, откуда его пытается выманить злоумышленник, например, по телефону.

В квартире около телефонного аппарата или на нем самом должны быть написаны номера служебных телефонов родителей, а также соседей или родственников (особенно тех, кто работает неподалеку), ближайшего отделения полиции и экстремальных служб города. Опыт показывает, что в напряженной обстановке даже взрослые не каждый раз могут вспомнить эти номера.

Ребенок не вернулся домой — это одна из самых драматических ситуаций, поэтому нужно делать все, чтобы его разыскать:

1) прежде всего, нужно сходить или позвонить туда, где он должен был быть, выяснить, кто его видел в последний раз, где и с кем; расспросить одноклассников, друзей, соседей;

2) проверить наличие документов и вещей пропавшего;

3) позвонить в справочные службы: "О заблудившихся детях", "О несчастных случаях", кроме того, узнать в больницах города, не поступал ли к ним ребенок с такими приметами;

4) сообщить в полицию по телефону "102" о пропаже;

5) если возникают подозрения относительно причастности к этому кого бы то ни было, сразу же информировать полицию;

6) начать с помощью соседей и родственников поиски в соседних дворах, подъездах, подвалах и на чердаках;

7) написать заявление на имя начальника отделения полиции с указанием примет пропавшего, приложить фотографию;

8) зарегистрировать заявление у оперативного дежурного;

9) не прекращать самостоятельных поисков, обращаться в общественные фонды и частный сыск;

10) в квартире в отсутствие родителей должен дежурить кто-то из соседей или родственников;

11) при возвращении ребенка сразу сообщить в полицию.

На наш взгляд, подробное изложение данной темы вызвано увеличивающимся числом террора со стороны преступных элементов в отношении не только бизнесменов (предпринимателей), но и членов их семей. Знание "азов" этой проблемы поможет предупредить в данной семье многие нежелательные явления.

Правила поведения при похищении

Стать заложником можно случайно, например, при ограблении банка, магазина, квартиры, загородного коттеджа, либо при захвате людей террористами.

Заложник — это человек, который находится во власти преступников. Сказанное не значит, что он вообще лишен возможности бороться за благополучное разрешение той ситуации, в которой оказался. Напротив, от его поведения зависит многое. Выбор правильной линии поведения требует соответствующих знаний. Таковыми должны обладать как сам бизнесмен, так и все члены его семьи.

Классическая схема похищения выглядит следующим образом: планирование, подготовка, захват, укрытие заложника, общение и допросы, ведение переговоров, получение выкупа, освобождение или убийство жертвы.

На этапе планирования террористы намечают объект для похищения, сумму предполагаемого выкупа, участников операции, наиболее подходящие места для похищения, ведения переговоров, получения выкупа.

Наиболее важными моментами этапа планирования являются выбор подходящей жертвы и определение суммы выкупа. Не всегда, например, в бизнесе, похищение связано с выкупом. Нередко таким способом пытаются получить какую-то важную информацию, заставить бизнесмена пойти на нежелательное для него сотрудничество, отказаться от реализации намеченных планов и т. д.

Превентивные меры защиты на этом этапе сводятся к осуществлению комплекса общих мер безопасности. Особое значение среди них имеют сокрытие информации о своем благосостоянии, маскировка и дезинформация, наличие личной охраны, проведение оперативной работы по выявлению потенциальных налетчиков.

На этапе подготовки террористы уделяют большое внимание детальному изучению образа жизни намеченной жертвы (и всех членов ее семьи), о тех местах, где они чаще всего бывают, о предпринимаемых мерах безопасности. Они проводят тщательное изучение местности, уточняют маршруты движения между домом, работой, другими посещаемыми местами, выясняют расположение помещений в квартире или офисе, сектор обзора из окон и т. д.

Изучают террористы и близких друзей, деловых партнеров, сотрудников объекта покушения. Это делается для определения тех лиц, которые могут оказаться полезными при ведении переговоров. Уточняют их имена и фамилии, адреса проживания, квартирные телефоны, марки и регистрационные номера личных автомобилей, приметы внешности для быстрого и точного опознания.

Захват является центральной частью операции. Анализ подобных акций, показал, что 90% всех похищений происходит в тот момент, когда жертва находится в пути на работу или с работы, недалеко от квартиры либо офиса. Иными словами, для захвата избирают обычно такое место, где невозможно изменить маршрут движения, даже если удается менять время приезда и отъезда.

Типовая акция по захвату осуществляется следующим образом. Один из террористов докладывает по радио или телефону о том, что объект покинул место работы (или квартиру), другой террорист сообщает, что автомашина объекта приближается к намеченному пункту. Здесь улицу блокируют специально подстроенным автомобильным инцидентом или перекрывают "внезапно сломавшимся" автофургоном (грузовиком).

Сам захват производится в тот момент, когда автомашина объекта останавливается у искусственно созданного препятствия. Здесь вступает в дело группа захвата, которая может скрываться в автомобиле, едущем за машиной объекта, маскироваться среди пешеходов или же находиться в автофургоне, блокировавшем улицу.

На открытых дорогах за городом преступники выступают в роли сотрудников ГИБДД, дорожных рабочих и т. д. Если имеется охрана, ее расстреливают, нейтрализуют электрошокерами, выводят из строя газовым оружием, дубинками. Независимо от того, на каком автомобиле увозят жертву с места события (ее собственном или на машине преступников), через несколько километров транспортное средство меняют на другое.

Похищение из дома — более сложная операция, так как оно связано с необходимостью проникновения в квартиру. Для этого террористы обычно маскируются под работников коммунальных, бытовых, ремонтных служб, сотрудников телеграфа, полицейских.

Еще более трудным считается похищение из внутренних помещений офиса, особенно, если там имеется охрана, предусмотрена блокировка дверей, есть сигнализация.

Как показывает практика, захват часто производится тогда, когда объект выходит из подъезда дома (офиса), направляясь к своему автомобилю, либо наоборот, выходит из автомобиля и направляется к себе домой (в офис).

При организации операций по захвату преступники стараются использовать в своих интересах устойчивые привычки поведения объекта похищения. Помимо привычек своих жертв, террористы стараются также использовать любые обстоятельства, помогающие им выиграть время и оттянуть момент обнаружения факта похищения.

В момент захвата террористы действуют бесцеремонно, даже жестоко. Нередко жертву лишают сознания ударом по голове, либо вводят объекту сильнодействующие медицинские препараты. Делается это для того, чтобы объект не сопротивлялся, не пытался убежать, не привлекал внимание посторонних людей и не мог понять, куда его везут. Для тех людей, которые плохо владеют своими эмо-

циями, наркотики в данном случае могут оказаться полезными, так как они снижают степень психического потрясения, успокаивают нервную систему, погружают в сон.

Однако гораздо чаще жертву просто лишают возможности двигаться, используя для этого веревку или наручники. Кроме того, глаза скорее всего залепят лейкопластырем, рот тоже. Сама транспортировка с места захвата вряд ли будет комфортной: обычно объект лежит на полу салона автомобиля под ногами похитителей, либо находится в багажнике. Может он очутиться в мешке, в ящике, бочке, даже в большом чемодане.

Некоторых людей в подобном положении охватывает приступ клаустрофобии (боязнь замкнутого пространства), сопровождающийся неприятными физиологическими ощущениями. Необходимо стойко перенести все неудобства, памятуя, что ситуация эта временная, максимум на несколько часов.

Реальная, в подавляющем большинстве случаев — единственная возможность вырваться из рук террористов бывает в начальной стадии захвата, в момент нападения. Неожиданные для террористов и решительные действия объекта нападения способны привести к спасению.

Отмечен ряд случаев, когда объекты нападения сбивали машиной нескольких террористов, открывали огонь из личного оружия, прорывались сквозь открытый по ним огонь и оставались в живых. Но если безуспешность попыток освободиться очевидна, лучше не прибегать к крайним мерам, а действовать сообразно складывающимся обстоятельствам.

С момента захвата необходимо контролировать свои действия и фиксировать все, что может способствовать освобождению. Надо постараться запомнить все детали транспортировки с места захвата: время и скорость движения, подъемы и спуски, крутые повороты, остановки у светофоров, железнодорожные переезды, характерные звуки.

По возможности все эти сведения надо постараться передать тем, кто ведет переговоры с террористами, — намеком или запиской. Понятно, что такого случая может не представиться, но в любом случае помните, что даже самая незначительная информация

о "тюрьме для заложника" может оказаться полезной для его освобождения, поимки и изобличения террористов.

Надо запоминать все увиденное и услышанное за время пребывания в заключении — расположение окон, дверей, лестниц, цвет обоев, специфические запахи, не говоря уже о голосах, внешности и манерах самих преступников.

Необходимо также наблюдать за их поведением, внимательно слушать разговоры между собой, запоминать распределение ролей. Короче, составлять в уме четкий психологический портрет каждого из них.

Известны случаи, когда похищенным людям удавалось оставлять в местах остановок условные знаки, выбрасывать наружу записки, тем или иным способом отмечать место своего заточения. Однако делать подобные вещи следует очень осторожно, так как в случае их обнаружения террористами неизбежно последует суровое наказание.

Человек становится жертвой с момента захвата, и хотя это происходит в разных условиях, жертва всегда испытывает сильное психическое потрясение (шок). Оно обусловлено внезапным резким переходом от фазы спокойствия к фазе стресса. Люди реагируют на такой переход по-разному: одни оказываются буквально парализованными страхом, другие пытаются дать отпор. Поэтому жизненно важно быстро справиться со своими эмоциями, чтобы вести себя рационально, увеличивая шансы на спасение.

Террористы "работают" с заложником так, чтобы максимально полно использовать его в своих интересах. Они всячески демонстрируют свое превосходство или власть над жертвой, даже если та не сопротивляется. Они стремятся подавить волю своего пленника и запугать его.

Поэтому заложник должен определить для себя позицию во взаимоотношениях с террористами. Как свидетельствует практика, безвольное поведение, мольбы о пощаде, сверхуступчивость реальной пользы принести не могут. Террористы в любом случае действуют исходя из своих планов и складывающихся обстоятельств.

Поэтому внешняя готовность к контакту с террористами и обсуждению интересующих их вопросов должна сочетаться с главным правилом: помогать не террористам, а себе. Ведь полученная от заложника информация в конечном счете используется во вред ему самому, его близким, сослуживцам, сотрудникам правоохранительных органов. Продуманно следует подходить к вопросам террористов о возможной реакции своего окружения на похищение, о сумме выкупа, о возможности удовлетворения других требований.

Сверхзадача здесь в том, чтобы своими ответами помочь людям, стремящимся найти и освободить заложника. В частности, аргументированное убеждение террористов в нереальности тех или иных требований может способствовать разрешению инцидента "малой кровью".

Террористы нередко находятся под воздействием наркотиков, в состоянии алкогольного опьянения.

Надо пытаться смягчить враждебность террористов по отношению к себе, искать возможности установления индивидуальных контактов с некоторыми из них. Это необходимо хотя бы для того, чтобы избежать физических страданий или улучшить условия содержания.

Но внешняя готовность найти общий язык с террористами, участие в обсуждении волнующих их проблем не должны противоречить упомянутому главному принципу: помогать себе, а не им.

И еще одна древняя истина может в ряде случаев принести пользу заложнику: разделяя — властвуй! Попытайтесь внести раскол в группу террористов, склоните кого-либо из них на свою сторону, обещая ему за это все, что вы можете реально пообещать.

Допрос. Практически всегда похищенных людей допрашивают. Допрос может иметь характер почти дружеской беседы, а может сопровождаться зверскими пытками.

Опытные террористы пытаются произвести впечатление дружеского расположения, что проливает бальзам на смятенную душу пленника, жаждущего психологической поддержки хотя бы на уровне эмоций.

Кроме того, ведущий допрос угрожает, что в случае неуступчивости жертвы он будет вынужден передать дело в руки своему помощнику, человеку жестокому и тупому. Поэтому, дескать, лучше не упираться зря, а пойти на сотрудничество. Старый трюк, но действенный!

Чтобы сломать заложника психологически, используют следующие меры давления:

— ограничивают подвижность (держат связанным либо в наручниках, на цепи), завязывают глаза и т. д.;

— мучают голодом и жаждой; лишают сигарет;

— создают плохие условия пребывания (теснота, грязь, вонь, шум, насекомые, сырость, холод, крысы и т. д.);

Для слабых натур уже всего перечисленного более чем достаточно, чтобы выполнить любые требования похитителей. Однако в запасе у террористов имеется еще такое средство, как *пытки.* За свою историю человечество разработало огромное количество пыток. Многие из них являются весьма действенными.

В целом пытки можно разделить на две основные группы: те, которые причиняют сильную боль и те, где главным средством воздействия является страх.

Первую группу составляют такие меры, как избиение, порка, сдавливание половых органов и нажатие на болевые точки, выкручивание суставов, сверление и вырывание зубов, порезы и разрывы кожных покровов, введение иголок, воздействие кипятком и раскаленными предметами, использование разрядов электрического тока и подобные им.

Вторая группа — это, в основном, угрозы удушения, утопления, нанесения обезображивающих повреждений лица, угроза изнасилования и так далее.

Как это ни странно на первый взгляд, пытки первой группы выдержать легче, чем второй. Дело в том, что существует так называемый "порог болевой чувствительности".

Стоит его превзойти, и организм отказывается воспринимать боль. Кроме того, известен психологический прием: если человек хочет вытерпеть физическое страдание, он расслабля-

ется и убеждает себя "полюбить боль", т. е. как бы превращается в мазохиста — извращенца, испытывающего наслаждение от ощущения боли.

Чтобы перенести меры психологического устрашения, требуется отсутствие внутреннего "Я" в данном месте в данный момент времени. А добиваться такого состояния мало кто умеет — нужна специфическая тренировка.

Поэтому, когда человеку одевают на голову пластиковый пакет или окунают с головой в ванну, он начинает задыхаться и впадает в состояние ужаса. Женщину легко запугать угрозой группового изнасилования либо демонстрацией попыток изуродовать ее лицо. Весьма эффективный способ "допросов с пристрастием" — когда при одном человеке подвергают пыткам другого. Особенно, если это близкие люди.

Руководствуйтесь следующими правилами.

• Перед каждым ответом на очередной вопрос делайте паузу подлиннее, чтобы понять, куда клонит преступник, а также для того, чтобы он не мог уяснить ваши слабые места. Паузы объясняйте тем, что вы вспоминаете подробности, думаете, как лучше сказать.

• Говорите, максимально используя профессиональные термины и любой известный вам специфический жаргон, чтобы вас меньше понимали.

• Старайтесь выражаться неясно, двусмысленно, многозначно.

• Побольше останавливайтесь на несущественных деталях, на разных мелочах, не имеющих прямого отношения к сути заданного вопроса.

• При каждом мало-мальски удобном случае повторяйте, что вы не располагаете нужной информацией, так как это не входило в сферу ваших обязанностей, интересов, компетенции.

• Притворяйтесь, что из-за боли, страха, волнения вы не способны собраться с мыслями, логично рассуждать.

• В некоторых случаях можно делать вид, будто вы не понимаете обращенных к вам вопросов из-за акцента преступника, использования им блатного жаргона, неясного произношения и т. д.

• Говорите монотонно, без эмоций, без жестикуляции, чтобы труднее было понять, где правда, а где ложь. Избегайте смотреть в глаза преступникам.

• Будьте вежливы в своей речи, не оскорбляйте бандитов, не говорите с ними о том, о чем они не хотят слышать, не спорьте, не критикуйте. Проводите свою линию не возражениями, а кажущимся согласием.

Сохранение психологической устойчивости при длительном пребывании в заточении — одно из важнейших условий спасения заложника. Здесь хороши любые приемы и методы, отвлекающие от неприятных ощущений и переживаний, позволяющие сохранить ясность мыслей, адекватную оценку ситуации.

• Старайтесь, насколько это возможно, соблюдать требования личной гигиены.

• Делайте доступные в данных условиях физические упражнения. Как минимум, напрягайте и расслабляйте поочередно все мышцы тела, если нельзя выполнять обычный гимнастический комплекс. Подобные упражнения желательно повторять не менее трех раз в день.

• Очень полезно во всех отношениях практиковать аутотренинг и медитацию. Подобные методы помогают держать свою психику под контролем.

• Вспоминайте про себя прочитанные книги, стихи, песни, последовательно обдумывайте различные отвлеченные проблемы (решайте математические задачи, вспоминайте иностранные слова и т. д.). Ваш ум должен работать. Верующие могут искать утешение в молитвах.

• Если есть такая возможность, читайте все, что окажется под рукой, даже если текст совершенно вам не интересен. Можно также писать, несмотря на то, что написанное будет отбираться. Важен сам процесс, помогающий сохранить рассудок.

• Важно следить за временем, тем более, что похитители обычно отбирают часы, отказываются говорить, какой сейчас день и час, изолируют от внешнего мира. Пишите календарь, отмечайте смену дня и ночи (по активности преступников, по звукам, по режиму питания и т. д.).

• Старайтесь относиться к происходящему с вами как бы со стороны, не принимая случившееся близко к сердцу, до конца надейтесь на благополучный исход. Страх, депрессия и апатия — три ваших главных врага, все они — внутри вас.

• Не выбрасывайте вещи, которые могут вам пригодиться (лекарства, очки, карандаши, платки и проч.), старайтесь создать хотя бы минимальный запас питьевой воды и продовольствия на тот случай, если вас надолго бросят одного или перестанут кормить.

Выкуп. Террористы отчетливо понимают, что наибольшей опасности они подвергаются в момент получения денежного выкупа. Поэтому они разрабатывают сложные, многоступенчатые системы передачи денег.

Цель принимаемых мер — исключение нападения из засады, фиксации факта передачи денег, установления личности террористов. Для этого террористы назначают время и место прибытия человека с деньгами, указывают маршрут, ведут скрытое наблюдение.

Курьеру могут предложить сесть в заранее подготовленный автомобиль и проехать в нем с сообщниками бандитов, затем его высаживают в удобном для них месте. Могут отвести в многоквартирный дом и получить деньги где-нибудь в подъезде, имеющем второй выход. Все время контакта ведется наблюдение за окружающими местами с целью выявления слежки.

Поскольку инициатива за террористами, они стремятся создать такие условия, которые не позволили бы сотрудникам полиции (если они задействованы) приблизиться на расстояние, с которого можно установить личность преступников либо захватить их. По тем же причинам они выбирают в качестве курьеров людей из ближайшего окружения заложника, облик которых им хорошо известен по этапу подготовки операции.

Получение выкупа не обязательно влечет за собой освобождение заложника. С ним могут расправиться для того, чтобы избавиться от возможного свидетеля. Кроме того, он может оставаться в руках бандитов до тех пор, пока они не реализуют полученные деньги.

Обычно деньги реализуют путем скупки драгоценностей, разных товаров, недвижимого и движимого имущества в регионах, удаленных от места совершения преступления. Иногда деньги стремятся вывезти за границу либо положить в банк на имя лиц, связи которых с преступниками сохраняются в тайне.

Освобождение. В том случае, когда террористы сами отпускают на свободу заложника, они отвозят его в какое-то безлюдное место и там оставляют одного. Другой вариант — его бросают в запертом помещении, выход из которого требует немало времени и сил. Третий вариант — высадить человека на оживленной улице и уехать. После этого машину вскоре бросают, либо меняют на ней номер.

Может случиться и так, что освобождать вас будет милиция. В этом случае надо пытаться убедить преступников, что лучше всего им сдаться. Тогда они могут рассчитывать на более мягкий приговор. Если подобная попытка не удалась, постарайтесь им внушить, что их судьба находится в прямой зависимости от вашей.

Если они пойдут на убийство, то всякие переговоры властей с ними теряют смысл. И тогда остается только штурм с применением оружия.

Когда террористы и заложники выходят наружу из убежища, им всем приказывают держать руки за головой. Не следует этим возмущаться, делать резкие движения. Пока не пройдет процедура опознания, меры предосторожности необходимы.

Если штурм начался или вот-вот начнется, попытайтесь прикрыть свое тело от пуль. Лучше всего лечь на пол подальше от окон и дверей, лицом вниз. В момент штурма не берите в руки оружие террористов. Иначе бойцы штурмовой группы могут принять вас за террориста и выстрелить на поражение. Им некогда разбираться в это время.

Террористы во время штурма нередко стремятся спрятаться среди заложников. Старайтесь в меру своих возможностей не позволять им этого делать, немедленно сообщайте о них ворвавшимся бойцам.

И последнее. В тех случаях, когда место содержания заложника установлено, спецслужбы стремятся использовать

имеющиеся у них технические средства для подслушивания разговоров, ведущихся в помещении.

Помните об этом и в разговоре с террористами сообщайте информацию, которая, будучи перехвачена, может быть использована для подготовки штурма. Особенно важны сведения о ярких и броских приметах, по которым можно отличить заложника от террористов, об их вооружении, количестве, расположении внутри помещения, их моральном состоянии и намерениях.

3.1.4. Преследование и захват автомобиля

Слежка за автомобилем предпринимателя может проводиться преступной группой с использованием нескольких машин. Обычно на задание выезжают в автомобилях, не привлекающих внимание окружающих.

Выявить слежку на автомобиле можно, неожиданно свернув в малолюдный переулок, быстро покинув автомобиль и наблюдая за поведением преследователей со скрытого поста.

Прежде всего необходимо уточнить, действительно ли это преследование.

Это можно выяснить, внезапно меняя направление движения или скорость, резко перестраиваясь из ряда в ряд, неожиданно останавливаясь, чуть отъехав от стоянки. И все это время следить за подозрительной машиной.

Если в автомобиле преступники, они вынуждены будут повторять все маневры преследуемой машины предпринимателя. Убедившись, что подозрения не напрасны, необходимо найти возможность связаться с полицией по телефону, с помощью работника автозаправки и т. д., но ни в коем случае не показывая, что слежка замечена. Таким же образом можно связаться и с друзьями, договориться о совместных действиях, в том числе о двойной слежке.

Для ухода от преследователей на автомобиле существует множество способов. Один из них — метод подсадки: после короткого отрыва вместо предпринимателя за руль садится человек, загримированный под него, а предприниматель пересаживается в дру-

гой автомобиль или уходит пешком. Этот метод особенно эффективен в темное время суток, а также при использовании автомобиля с тонированными стеклами.

Следует учесть, что преследователи могут отслеживать движение объекта с помощью радиомаяков, установленных на автомобиль предпринимателя. Для противодействия этому виду слежки можно использовать операцию "чистый автомобиль".

Если за предпринимателем следят, не следует совершать "противозаконные" действия — переезд через сплошную линию разметки, игнорирование светофора. Это может привлечь внимание не только сотрудников полиции, но и преследователей, которые, как показывает практика, нередко в этих случаях провоцировали аварии или портили автомобиль на стоянке.

Старайтесь, по возможности, избегать постоянных маршрутов при поездках на работу и с нее. Опыт показывает, что преступники обычно держат свою жертву под наблюдением, чтобы выбрать наиболее подходящее место и время для нападения. Выберите хотя бы четыре разных маршрута и пользуйтесь ими по принципу случайного выбора. Непредсказуемость — ваша лучшая защита.

Старайтесь ездить по оживленным дорогам, избегать пустынных улочек и проселочных дорог. Проверяйте, не преследует ли вас какой-то автомобиль. При движении по многорядному шоссе занимайте место в среднем ряду, чтобы не дать возможности прижать ваш автомобиль к обочине.

Когда едете в машине, закрывайте все двери на кнопки. Если вас остановили (например, ГИБДД), не выходите из машины, во всяком случае, если место пустынное, а время суток темное. Машину держите на передаче, чтобы иметь возможность в любой момент дать газ.

Если машина с террористами перегородила вам путь (чаще всего в таких случаях используют "ножницы" — одна машина перекрывает дорогу спереди, другая — сзади), на большой скорости бейте в место, соответствующее одной трети машины (сразу за передним колесом или перед задним). Ни в коем случае не останавливайтесь. Если местность позволяет, уходите на скорости по обочине, по бездорожью.

Если террорист готовится начать стрельбу по вашей машине, увеличивайте скорость и направьте автомобиль прямо на него. От пуль укройтесь, пригнувшись ниже лобового стекла, но продолжая держать руль руками в избранном направлении. Сбив террориста машиной, не тратьте время на выяснение того, в каком он состоянии. Немедленно уезжайте на максимальной скорости.

Необходимо, чтобы все места в автомобиле (а не только передние) были снабжены ремнями безопасности. Желательно также укрепить салон изнутри дополнительным ребром жесткости, исключающим сплющивание в случаях падения под откос или тарана. Вообще говоря, при желании автомобиль любой марки можно так оборудовать для "войны на дорогах", что он станет своего рода "броненосным крейсером". И тогда вы сметете с пути любой автомобиль, кто бы им ни управлял.

Если в салон автомобиля забросили бутылку с зажигательной смесью, не останавливайтесь. Температура внутри салона не поднимется выше 55–60 °С, а такая температура не опасна для жизни. На предельной скорости уходите от места происшествия — ведь бутылку бросили именно для того, чтобы "выкурить" вас из машины. Если хотят уничтожить, то бросают гранату типа Ф-1, а сам преступник немедленно скрывается.

Но есть и иная опасность, которая может грозить предпринимателю, когда он за рулем автомобиля: разбойное нападение с целью завладения автомобилем, а заодно и документами к нему. Как уберечься от такого рода экстремальной ситуации? Как выбраться из нее, если она все-таки настигла?

Машины часто угоняют для продажи, для разукомплектования и продажи запчастей, по заказу, при этом может быть оговорена не только марка или сохранность автомобиля, но даже его цвет.

Профессиональные угонщики тщательно организуют свою деятельность, страхуют друг друга и четко перераспределяют свои криминальные роли. В их руках специальная техника (в том числе и противосигнализационная) и великое разнообразие приемов.

Однако немалая часть угонов все-таки осуществляется дилетантами, и если защитить свой автомобиль хотя бы от них, то вероятность кражи резко уменьшается.

В систему угона входит слежение за хозяином машины (распорядок дня, отключение сигнализации и возможных автохитростей, о которых, как правило, узнают, когда предлагают услуги в ремонте, при открывании капота и т. п.).

Против сигнализации используют несколько приемов. Воры играют на нервах, раскачивая по ночам нужную машину, пока владелец сам не отключит сигнализацию. Другие используют электрошок для выведения сигнализации из строя. Третьи согнутой проволокой, залезая под днище, обрывают провода сигнализации.

Некоторые используют обычный радиоприем для определения частоты радиосигнала при включении и выключении сигнализации хозяином. После этого генератором подают сигнал нужной частоты, чтобы отключить сигнализацию "нужного" автомобиля.

Еще чаще используется быстрота рук: ворвавшись в салон, злоумышленник открывает запоры капота и снимает в мгновение ока одну из клемм аккумуляторной батареи, а потом уже отключает сигнализацию.

Проникновение в машину преступники осуществляют несколькими способами:

1) подбирают ключи к дверям, багажнику;

2) отжимают, снимают или выдавливают стекла (обычно снимают задние стекла, выдавливают боковые форточки, отжимают вниз стекла дверей);

3) открывают двери с помощью тонкой металлической пластины, просунутой между стеклом двери и уплотнением.

Завести машину не составляет никакого труда, соединив клеммы от замка зажигания.

Если заблокирован руль, то воры ломают язычок замка резким движением руля в одну и другую стороны.

Для того чтобы предупредить захват и угон автотранспорта, необходимо воспользоваться некоторыми советами.

1. Прежде всего необходимо обзавестись надежным противоугонным устройством, поставить надежные замки на двери и ба-

гажник. Закрепить кожух, прикрывающий тяги замка от отпирания с помощью линейки или металлической пластины.

2. Ставится дублирующая скрытая сигнализация на случай отключения открытой для посторонних глаз.

3. Делается гравировка на наиболее "уязвимых" частях: на лобовом и заднем стеклах, фарах, подфарниках, дисках колес и кодируются специальной краской основные узлы машины, надписи кода видны только при инфракрасном облучении.

4. Записываются номера всех покрышек, радиоприемника и магнитолы.

5. На бензопроводе монтируется потайной электроклапан или вентиль, который перекрывает на стоянке подачу топлива.

6. Ставится потайной выключатель на один из проводов катушки зажигания.

7. Ставятся блокировочные устройства на руль, педали, рукоятку переключения скоростей.

8. На колеса ставятся болты (хотя бы один) с нестандартными ("секретными") головками (вращающимися, эксцентрическими и т. п.).

9. На горловину бензобака надевается крышка с замком, исключающая всякие неприятности, в том числе использование террористами.

10. Есть и более экзотические средства: электрошоковый коврик на сиденье водителя (мощность — 40 киловольт), минирование с использованием газовых устройств и т. п.

11. Рекомендуется на ночь снимать крышку трамблера, бегунок трамблера или центральный провод, который соединяет катушку высокого напряжения с трамблером.

Что следует делать в целях снижения риска хищения автомашины?

Большинство разноплановых рекомендаций касается внешнего вида автомобиля. Нарядный автомобиль всегда привлекает воров. Всякие "навороты" на корпусе автомашины, дополнительные устройства, антенны и т. п. дают много информации о ее хозяине и его возможностях.

Не рекомендуется ставить машину в затемненных местах.

Не нужно в багажнике хранить много дополнительного бензина.

В салоне не должны оставаться какие-то вещи, сумки, что привлекает внимание посторонних.

Документы на автомашину, ключи следует всегда хранить при себе и ни в коем случае не оставлять в машине, даже если она находится в гараже.

Если предприниматель заметил рядом со своим автомобилем подозрительных людей, не стоит рисковать.

Если он выходит из подъезда дома, можно использовать нехитрый прием информационной защиты — обернуться и крикнуть в подъезд что-нибудь вроде: *"Спускайтесь все! Уедем на двух машинах!"*

Не стоит кидаться под колеса, когда машина уже тронулась или еще стоит, но в ней сидят злоумышленники. Основная задача — вызвать полицию и блокировать выезд. В крайнем случае хозяину остается разбить лобовое стекло своей машины камнем, запомнить приметы преступников и направление движения, а затем опять же звонить в полицию.

Все вышеприведенные возможные пути угроз здоровью и жизни предпринимателя говорят об увеличении вероятности теракта, а из этого следует, что до тех пор пока существует источник опасности в лице отдельной группы людей или конкретной личности, заинтересованной в этом, опасность будет сохраняться до полной развязки.

В этом случае необходимо проанализировать вероятные причины возникших угроз: неуплата долга, отклонение требований рэкетиров, конкуренция, бытовые проблемы и прочее.

Исходя из вероятных причин угрозы теракта, необходимо выявить источник опасности. Одновременно с усилением мер личной безопасности, т. е. введением иного режима безопасности (особые мероприятия на рабочем месте; при нахождении на улице (в транспорте); при возвращении домой и нахождении в квартире) необходимо продумать личную информационную защиту, в том числе дезинформацию преступников.

3.1.5. Защита семьи предпринимателя от разбоя и теракта в квартире

Оградить свое жилище от квартирных воров можно разными способами.

Во-первых, необходимо, чтобы все места, через которые преступники проникают в квартиру, были надежно укреплены, прочны и имели бы надежные запорные устройства.

Для окон, балконных дверей, которые имеют остекленные поверхности, необходимо, чтобы оконный переплет был прочным, задвижки и шпингалеты должны быть надежно укреплены и могли бы закрываться на их полный ход. Там, где есть возможность легко проникнуть в окно, на лоджию (балкон), устанавливаются балконные решетки.

Существенно осложняют возможность проникновения в помещение правильно установленные двойные двери, открывающиеся в разные стороны, а также монолитная дверь, имеющая усиленный край.

Оптимальным, как показывает практика, является одновременное использование для запирания дверей двух замков разной конструкции: одного — врезного с сувальдным механизмом, затрудняющим проникновение путем взлома или отжима, другого — с цилиндровым механизмом, имеющим более высокую степень защиты от отпирания их посторонними людьми.

По мнению специалистов, наиболее надежными являются штифтовые цилиндрические замки, имеющие от трех до семи штифтов.

Проверенным средством защиты является применение замков с перемещением язычка без использования пружины. Открыть такой замок, просунув пластину из негнущегося материала между краем двери и обвязкой дверной коробки, невозможно. Существуют и другие конструкции замков, отличающиеся высокой степенью надежности, поэтому, прежде чем принять решение об установке одного из них, рекомендуется воспользоваться советом специалиста.

Не следует забывать о надлежащей защите всех без исключения входных дверей, особенно тех, что ведут на черный ход, который, как правило, имеют загородные дома, дачи. Учитывая, что многие взломщики предпочитают проникать в дом именно с черного входа, рекомендуется не только закрывать его на замок, но и запирать на засов. Для большей уверенности засов запирается навесным замком.

Одним из существенных препятствий в подъездах домов для преступников являются замочно-переговорные устройства, называемые домофонами. Основные их типы — "Сезам", "Визит", "Диалог".

Помимо домофонов, может использоваться видеозвуковая система опознания посетителей в жилых домах. Мини-видеокамера позволяет наблюдать даже в темноте, отображая изображение на бытовом телевизоре. Камера включается при нажатии посетителем дверного звонка.

Предприниматель (бизнесмен) должен осуществить имущественное страхование с целью возмещения потерь, причиненных стихийными бедствиями, несчастными случаями и иными обстоятельствами, в том числе в результате хищения.

Практика показывает, что сегодня самый эффективный способ уберечь личное имущество от хищения — передача его под охрану отделам вневедомственной охраны. Даже если вор успеет уйти, ущерб будет возмещен.

При утере ключей, даже если их вернули, необходимо менять все замки вместе с ключами. Это исключает возможность кому-либо постороннему беспрепятственно проникнуть в квартиру.

Чтобы избежать разбоя в квартире (а подавляющее большинство ограблений — групповые), нужно сформировать у себя и домашних несколько полезных привычек:

1. Никогда не открывать дверь не известному лично вам человеку. Чтобы убедиться, что перед вами действительно милиционер, позвоните в свое отделение полиции. Вы имеете право не впускать посторонних в квартиру, исключение — чрезвычайное положение в городе или наличие ордера, но вы вправе требовать присутствия понятых из известных вам соседей.

О визите слесаря, которого вы не вызывали, также можно узнать, позвонив в домоуправление.

Если из-за двери объясняют, что возникла острая необходимость позвонить по телефону, скажите, что сделаете это сами — спросите номер и что передать.

Если вам кажется, что стоящий за дверью действительно нуждается в помощи, свяжитесь по телефону с соседями и выходите на площадку одновременно с ними (кстати, номера телефонов соседей всегда должны быть под рукой, лучше всего записать их на бумажке, приклеенной к самому аппарату).

2. Никогда не открывайте дверь, если в глазок никого не видно, если погас свет. Позвоните соседям, выясните ситуацию: глазки нескольких квартир могут специально заклеить, электричество в доме могут умышленно испортить; злоумышленник может прятаться за углом и звонить несколько раз, делая вид, что это балуются дети.

3. Никогда не открывайте дверь, не посмотрев в глазок, далее если ждете детей из школы или гостей (одна из подмосковных банд, грабившая "по наводке", выбирала именно те дни, когда их состоятельные жертвы ждали гостей).

4. В случае вероятности теракта (по ранее выявленным признакам) категорически запрещается смотреть в глазок даже в бронированной двери, так как преступник может выстрелить в хозяина, услышав его голос: *"Что вам нужно?"*

Если дверь кто-то пытается открыть, не торопитесь кричать через дверь, что вы все слышите — не теряйте своего информационного преимущества. Будучи уверенным, что ваша дверь достаточно крепка, закрыта на внутреннюю щеколду, засов и т. д., без промедления звоните в полицию. Позвоните соседям, попросите посмотреть, кто и что делает у вашей двери, пусть соседи запомнят приметы.

При удачном стечении обстоятельств можно попытаться задержать вора или злоумышленника, действуя как группа соседской взаимопомощи и используя свое право на необходимую оборону.

Если же есть сомнения в прочности двери, первым делом надо блокировать вход любыми тяжелыми предметами, даже просто завалить его одеждой и вещами.

Если злоумышленники рвутся в квартиру открыто, немедленно поднимите тревогу: стучите тяжелыми предметами по батарее, кричите, разбейте окно, обратитесь к людям на улице, чтобы вызвали полицию и помогли вам. Выбегайте на балкон. Попытайтесь вызвать полицию сами. Приготовьтесь активно отражать нападение.

Если есть собака, используйте и ее (даже как отвлекающий фактор).

Если попытки проникнуть в квартиру прекратились, не спешите выходить — вас могут ждать. Свяжитесь с соседями, с полицией, посмотрите в окно — не выходят ли из вашего подъезда незнакомцы. Их приметы, а также марку, цвет и номер машины, куда они уходят, надо запомнить (лучше тут же записать) и передать полиции.

Безусловно, на все случаи жизни невозможно дать готовые рецепты, а тем более связанные с предупреждением разбойных нападений, терактов. На наш взгляд, изложенный подход к этой проблеме позволит по-иному оценивать свою безопасность и правильно принимать решение по ее организации.

3.1.6. Защита автомобиля, квартиры от террористического акта

Перед тем, как садиться в машину, необходимо произвести внешний осмотр: состояния колес, запоров, нет ли видимых следов открывания дверей, нет ли кого в салоне. Дополнительные провода под машиной, в багажнике, моторном отсеке могут явиться результатом установки мины и взрывного устройства.

При обнаружении подозрительного предмета под машиной рекомендуется его не трогать до прибытия специалистов по обезвреживанию взрывных устройств.

Очень часто преступники, выполняющие заказное убийство, используют простейший прием минирования машины: граната или

связка гранат привязывается к автомобилю. В кольцо чеки продевают леску, конец которой прикреплен к неподвижному предмету рядом с машиной. Автомобиль трогается, предохранительная чека выдергивается из гнезда.

Какие меры противодействия наиболее эффективны, если возникают опасения, что автомобиль может быть заминирован?

Прежде всего нужно быть предельно собранным, не оставлять без внимания ни одной мелочи. В таком случае хороший эффект дают, казалось бы, самые простые методы информационной защиты, такие, например, как установка в салоне и на капоте своих маленьких секретов (обломок спички в определенном месте или приклеенный волосок).

Если такая "сигнализация" нарушена, не заводите машину, осмотрите ее и при малейшем подозрении обращайтесь к специалистам.

Должно насторожить и отсутствие части грязевого слоя на днище автомашины.

Угроза взрыва не ограничивается автомобилем. Нередко взрывные устройства устанавливаются у входной двери в квартиру или на дачном участке. Здесь тоже, прежде чем войти, стоит проявить бдительность.

Подозрение должны вызвать:

1) следы ремонтных работ у входа в квартиру, площади с нарушенной окраской, поверхность которых отличается от общего фона;

2) сумка, портфель, коробка или какой-либо предмет, которые в этом месте не оставлялись;

3) на даче — выделяющиеся участки свежевырытой или высохшей земли.

Современные взрывчатые вещества (типа пластита, семтекса) и средства взрывания позволяют специалистам, имеющим армейскую подготовку, конструировать самые разнообразные миниатюрные мины-ловушки. К счастью, среди преступников таковых мало, поэтому они применят в большинстве случаев кустарные взрывные устройства.

Для покушения может использоваться и почтовый канал. Взрывные устройства, направляемые в письмах, используются не для убий-

ства, а для устрашения получателя. Ведь 20–40-граммовый заряд взрывчатки может нанести, как правило, только ранение и вызвать сильный шок. Для уничтожения применяют не письма, а бандероли и посылки.

Взрывные устройства, которые закладывают в конверты, бандероли и посылки, могут быть как мгновенного, так и замедленного действия. Взрыватели мгновенного действия вызывают срабатывание взрывного устройства при нажатии, ударе, прокалывании, снятии нагрузки, разрушении элементов конструкции, просвечивании ярким светом и т. д.

Например, взрывные устройства, действующие по принципу музыкальной открытки, взрываются при их раскрытии. Взрывные устройства в бандеролях срабатывают либо при открывании, либо при попытке извлечь книгу или коробку из упаковки. Взрывные устройства в посылках обычно срабатывают при вскрытии крышки посылочного ящика.

Взрыватели замедленного действия по истечении заранее установленного срока (от нескольких часов до нескольких суток) либо вызывают взрыв, либо приводят взрывное устройство в боевое положение, после чего срабатывание взрывного устройства происходит мгновенно в случае внешнего воздействия на него.

Независимо от типа взрывателя и взрывного устройства, письма, бандероли и посылки с подобной начинкой неизбежно обладают рядом признаков, по которым можно их отличить от обычных почтовых отправлений. Эти признаки делятся на основные и вспомогательные.

К числу основных признаков относят следующие:

1) толщина письма от 3 мм и выше, при этом в нем есть отдельные утолщения;

2) смещение центра тяжести письма (пакета);

3) наличие в конверте перемещающихся предметов или порошкообразных материалов;

4) наличие во вложении металлических либо пластмассовых предметов;

5) наличие на конверте масляных пятен, проколов, металлических кнопок, полосок и т. д.;

6) наличие необычного запаха (миндаля, марципана, жженой пластмассы и других);

7) "тикание" в бандеролях и посылках часового механизма (один из самых простых и распространенных взрывателей делают с помощью обычного будильника);

8) в конвертах и пакетах, в посылочных ящиках при их переворачивании слышен шорох пересыпающегося порошка.

Наличие хотя бы одного из перечисленных признаков (а тем более сразу нескольких) позволяет предполагать присутствие в почтовом отправлении взрывной "начинки".

К числу вспомогательных признаков относятся:

1) особо тщательная заделка письма, бандероли, посылки, в том числе липкой лентой, бумажными полосами и т. д.;

2) наличие надписей типа "лично в руки", "вскрыть только лично", "вручить лично", "секретно", "только директору (владельцу, председателю)" и т. д.;

3) отсутствие обратного адреса или фамилии отправителя, неразборчивое их написание, явно вымышленный адрес;

4) самодельная нестандартная упаковка.

Сказанное здесь о посторонних предметах, остатках изоляции, о проводах и проч. имеет значение и в отношении офиса, квартиры, дачи, подъезда, даже обычной входной двери.

Как и во множестве других случаев, профилактические меры в защите от терактов оказываются наиболее эффективным средством, хотя надо признать, что идеальных средств тут нет вообще.

При увеличении вероятности теракта (угрозы, шантаж, замеченная слежка) необходимо не просто внимательнее выполнять меры предосторожности, а ввести иной уровень режима личной безопасности — от информационной защиты, особых мероприятий на рабочем месте, в транспорте и жилье, вплоть до смены места жительства.

В любом случае в этот период, когда угроза становится реальной, необходимо обратиться к специалистам для проведения зачистки объектов, где чаще всего бывает или находится предприниматель.

В процессе зачистки объекта в первую очередь следует искать:

1) взрывные устройства;

2) взрывчатые и воспламеняющиеся вещества;

3) химические отравляющие вещества;

4) радиозакладки подслушивания и дистанционного управления минами и т. п.

Проведение зачистки проводится с использованием специальных приборов и собак. После зачистки, как правило, выставляется постоянная охрана объекта (офиса, квартиры, дачи, автомашины и т. п.).

Устанавливается особый режим личной безопасности и для членов семьи предпринимателя, который отменяется с ликвидацией источника угрозы.

3.1.7. Порядок принятия решения и разработки плана организации системы безопасности и защиты фирмы, ее ведущих сотрудников

Руководитель фирмы выбирает направление действий не только для себя, но и для организации и других работников.

Ответственность за принятие важных организационных решений — тяжелое моральное бремя, что особенно ярко проявляется на высших уровнях управления. Непродуманное решение может привести к катастрофическим последствиям.

Организационные решения можно квалифицировать как запрограммированные и незапрограммированные.

Запрограммированное решение есть результат определенной последовательности шагов или действий, подобных тем, что предпринимаются при решении математического уравнения. Как правило, число возможных альтернатив ограничено и выбор должен быть сделан в пределах направлений, заданных организацией.

К примеру, вы решили на всех важных объектах вашей фирмы, помимо технических средств контроля, поставить по одному посту физической охраны. Если на каждом посту должно быть не менее 2 человек, а в каждом здании вашей фирмы имеется по два

таких объекта, то решение принимается автоматически — в 10 зданиях ежедневно должно быть 40 охранников, поскольку они несут службу через два дня на третий, всего должно быть 120 охранников.

Незапрограммированные решения требуются в ситуациях, которые в определенной мере новы, внутренне не сконструированы или сопряжены с неизвестными факторами. Поскольку заранее невозможно составить конкретную последовательность необходимых шагов, руководитель должен разработать процедуру принятия решения.

К числу незапрограммированных можно отнести решения следующего типа: какими должны быть цели службы безопасности в дневное (рабочее) время и в вечернее (нерабочее) время, каким образом должны действовать охранники в экстремальных условиях в эти периоды, как усилить меры защиты фирмы, как усовершенствовать организацию службы безопасности, как усилить мотивацию сотрудников службы.

В каждой из подобных ситуаций (как чаще всего бывает с запрограммированными решениями) истинной причиной проблемы может быть любой из факторов. В то же время руководитель располагает множеством вариантов выбора.

Это может быть выбор интуитивного решения, его иногда называют озарением или шестым чувством. Чаще делается выбор решения, основанного на суждениях, обусловленный знаниями или накопленным опытом.

Человек использует знание о том, что случалось в сходных ситуациях ранее, чтобы спрогнозировать результат альтернативных вариантов выбора в существующей ситуации. Опираясь на здравый смысл, он выбирает альтернативу, которая принесла успех в прошлом.

Адаптация к новому и сложному, очевидно, никогда не будет простым делом. Нельзя исключить опасность неудачи из-за принятия плохого решения. Однако во многих случаях руководитель в состоянии существенно повысить вероятность правильного выбора, подходя к решению рационально.

Главное различие между решениями рациональным и основанным на суждении заключается в том, что первое не зависит от прошлого опыта. Рациональное решение обосновывается с помощью объективного аналитического процесса, так как речь идет о нескончаемой последовательности взаимосвязанных шагов.

Для принятия решения необходимо провести оценку ситуации или стоящей проблемы, чаще менеджеры используют термин "диагностика проблемы", военные — "оценка обстановки". Как правило, для выявления причин возникновения проблемы необходимо собрать и проанализировать требующуюся внутреннюю и внешнюю (относительно организации) информацию.

Такую информацию можно собирать на основе формальных методов, используя, например, вне организации анализ рынка, а внутри нее — компьютерный анализ финансовых отчетов, интервьюирование, приглашение консультантов по управлению или опросы работников.

Получение информации также возможно путем анализа периодической печати, местных радио-, телепередач и газет, что позволяет правильно оценивать политическую, экономическую и криминогенную обстановку в стране, регионе, области, районе и городе, а также влияние всех внешних факторов на положение фирмы на рынке сбыта и производства.

Изучение морально-психологического климата в трудовом коллективе позволяет определить, благотворно ли он влияет на надежность и стабильность производства или снижает надежность, дестабилизирует производство, а также приводит ли к снижению или увеличению рисков.

Информацию можно собирать и неформально, ведя беседы о сложившейся ситуации и делая личные наблюдения. Начальники цехов, мастера могут обсудить проблему безопасности и защиты фирмы с рабочими и передать полученную информацию наверх.

Увеличение количества информации не обязательно повышает качество решения. Поэтому в ходе наблюдения, бесед важно видеть различия между релевантной (относящейся к делу) и неуместной информацией и уметь отделять одну от другой.

Поскольку релевантная информация — основа решения, естественно добиваться по возможности ее максимальной точности и соответствия проблеме.

Руководитель обобщает информацию и оформляет ее документально, так как этот документ является одним из самых важных при принятии решения, особенно в нашем частном случае.

Решение руководителя крупного предприятия (фирмы) об организации систем безопасности и защиты предприятия должно содержать:

1. Задачи службы безопасности.

2. Выводы из оценки обстановки:

1) положение на рынке услуг (производства);

2) основные группировки сил конкурентов, преступных элементов (их построение, способы действий, возможности);

3) основная угроза фирме;

4) силы СБ фирмы, ее состав, возможности;

5) особенности ситуации в стране, городе (месте дислокации фирмы) и ее влияние на рынок услуг и производства, положение фирмы.

3. Задачи, решаемые службами безопасности соседних предприятий в интересах фирмы.

4. Задачи, решаемые силами и средствами МВД в интересах фирмы.

5. Указания по взаимодействию с МВД и другими службами безопасности.

6. Организация развертывания и усиления сил СБ фирмы, техническое и материальное обеспечение их деятельности.

7. Указания (план) по организации управления силами СБ фирмы в экстремальных ситуациях (по вариантам).

8. Срок готовности сил СБ к выполнению функциональных обязанностей в полном объеме.

Рассмотрим более подробно каждый этап по подготовке и принятию решения.

I. ***Оценка обстановки.***

Рассмотрим порядок принятия решения руководителем (предпринимателем) об организации системы безопасности и защиты фирмы, ее ведущих специалистов на условном примере.

Пример. Фирма "Золотой якорь" занимается импортом подержанных и новых автомобилей ведущих фирм Западной Европы, а также производит их ремонт и продает на внутреннем рынке. Кроме этого, для полной загрузки авторемонта и автостоянки принимаются заказы на обслуживание отечественных и импортных автомобилей частных лиц и организаций, а также предоставляется возможность проката автомобилей на короткий срок с последующей продажей и без продажи.

Для выполнения всех функций в состав фирмы входят: автостоянка на 150 мест для легковых и 50 мест для грузовых автомобилей; автосервис (ремонтная база, склад, мойка, цех по покраске); бензозаправка; автомагазин; кафе; двухэтажный офис со всеми службами безопасности и соответствующим оборудованием).

Общие сведения:

1) площадь территории фирмы 3 гектара, расположена перед въездом в город;

2) штат: 6 человек управления, 36 человек рабочих и служащих;

3) ежемесячная чистая прибыль составляет 120 млн у. е.

За последние три месяца политическая и экономическая обстановка в стране обострилась в связи с нестабильностью в некоторых соседних странах и ростом инвестиций в восстановление их экономик, что привело к значительному повышению цен на продукты первой необходимости, сырье и т. п. Увеличены налоги с предприятий. На межгосударственном уровне стали более прохладными отношения с прибалтийскими странами, через которые шли поставки автомобилей из Скандинавии; в последнее время их поток уменьшился из-за предвзятости таможенных служб Латвии и Эстонии. Фирма терпит убытки из-за нарушения договорных обязательств.

За последний месяц задержана зарплата рабочим фирмы из-за нестабильного финансового положения.

Нарастает предвыборная борьба по выдвижению кандидатов в Госдуму. По сообщениям МВД, в списках кандидатов более 30 человек, имевших ранее судимости.

Сезонные работы в сельской местности закончились, в области, городе многие предприятия не работают, большинство рабочих находится в вынужденных отпусках с получением минимальной заработной платы, поэтому значительно обострилась криминогенная обстановка. Как свидетельствуют местная пресса, радио и телевидение, увеличилось число разбойных нападений, хищений и т. п.

По докладам сторожей, 21 августа и 15 сентября со склада запасных частей фирмы похищены дефицитные запчасти на общую сумму 15 500 долл. На автозаправке уже несколько раз по принуждению рэкетиров были заправлены автомашины без номеров.

Все это привело к нездоровой обстановке в компании, два ведущих специалиста подали заявления об увольнении, считая, что фирма на грани развала.

Появились претензии клиентов на брак в работе, хищения дворников, зеркал, колпаков и т. п. на стоянках. Сторожа не справляются с поставленной задачей из-за большой протяженности территории автостоянки и наличия значительных материальных ценностей.

Выводы из оценки обстановки:

1. В ближайшие несколько месяцев экономическая и политическая ситуация в стране радикально не изменится.

В связи с ухудшением жизненного уровня населения города возможны увеличение количества краж, более решительные действия преступных группировок из-за отвлечения большого числа городской полиции в командировки в проблемные страны (необходимо учитывать и отдаленность фирмы от города).

Из-за того, что фирма находится в более выгодном финансовом положении по сравнению с предприятиями города и конкурентами, возможен рэкет.

2. ЧП, связанные с хищением имущества фирмы на крупную сумму, показывают слабость охраны многих объектов фирмы, особенно тех, где наибольший интерес для воров представляют большие материальные ценности.

3. Большая территория не позволяет сторожам эффективно решать вопросы охраны, из-за отсутствия спецсредств, подготовки, малочисленности состава охраны и отсутствия технических средств контроля и раннего предупреждения.

4. Слабая дисциплина труда и постоянная утечка коммерческой информации привлекают внимание преступных элементов. Требуется принять срочные меры по перекрытию этих каналов и смена мест хранения материальных ценностей или усиления их охраны.

5. Необходимо усилить охрану стоянок, бензозаправки, склада, а также других структур фирмы, могущих стать объектом внимания преступных элементов и группировок.

6. Следует создать службу безопасности фирмы или обратиться к предприятию, выполняющему охранные функции.

7. Продумать меры по снижению риска воздействия на фирму преступных элементов и группировок.

II. ***Формулировка ограничений и критериев принятия решения.***

Подготовив анализ обстановки и сделав из него выводы, руководитель фирмы должен отдавать себе отчет о том, что именно можно с ним сделать. Многие возможные решения проблем фирмы не будут реалистичными, поскольку либо у руководителя, либо у организации недостаточно ресурсов для реализации принятых решений.

Кроме того, причиной проблемы могут быть находящиеся вне организации силы — такие, как законы, которые руководитель не властен изменить. Перед тем, как переходить к следующему этапу процесса, руководитель должен беспристрастно определить суть ограничений и только потом выявлять альтернативы.

Если этого не сделать, как минимум, будет впустую потеряна масса времени. Еще хуже, если будет выбрано нереалистичное направление действий. Естественно, это усугубит, а не разрешит существующую проблему.

Ограничения зависят от ситуации и конкретных руководителей. Некоторые общие ограничения на нашем примере — это неадекватность средств; недостаточное число охранников, имеющих требуемую

квалификацию и опыт; неспособность в короткий срок закупить все охранное оборудование и отсутствие специалистов по его монтажу; законы и этические соображения и др.

Кроме идентификации ограничений, руководителю фирмы необходимо определить стандарты, по которым предстоит оценивать альтернативные варианты выбора. Эти стандарты принято называть критериями принятия решения. Они выступают в качестве рекомендации по оценке решений.

Рассмотрим наш пример.

Основные требования к службе безопасности фирмы:

1) общий расход средств на содержание технических и физических средств охраны не должен превышать 15–20% чистой прибыли фирмы;

2) количество технических средств охраны (контроля) и численность сотрудников СБ не должны превышать разумной потребности;

3) все сотрудники СБ должны иметь лицензию на выполнение охранных функций;

4) руководитель СБ должен иметь высшее образование;

5) СБ фирмы должна обеспечивать выполнение всех функций, определенных в Уставе службы безопасности.

III. ***Формирование набора альтернативных решений проблемы.***

С этой целью руководитель фирмы дает указания всем ведущим специалистам предприятия подготовить свои предложения для принятия решения.

Помимо этого, если не решен вопрос создания СБ фирмы, руководитель должен воспользоваться услугами охранных предприятий по разработке предложений для решения вопросов обеспечения безопасности и защиты его фирмы.

Можно воспользоваться опытом сотрудничающих предприятий и идентичных с фирмой предприятий в других городах и т. п.

IV. ***Оценка альтернатив.***

Предпринимателю может быть предложено несколько вариантов охраны:

1) заключить договор об абонементном обслуживании охранным предприятием;

2) заключить договор с полицией об охране с помощью технических средств;

3) нанять сторожей и выставить сторожевых собак;

4) организовать собственную охранную службу (службу безопасности);

5) другие варианты и сочетания.

Это означает, что только после составления списка всех идей следует переходить к оценке каждой альтернативы. При оценке решений руководитель определяет достоинства и недостатки каждого из них и возможные общие последствия.

Для сопоставления решений необходимо располагать стандартом, относительно которого можно измерить вероятные результаты реализации каждой возможной альтернативы.

В нашем примере мы предложили воспользоваться помощью охранных предприятий, предлагающих услуги безопасности, — безусловно, на договорной основе. Их вариант решения по обеспечению безопасности и защиты фирмы, ее ведущих сотрудников может быть избран в качестве стандарта, так как он будет адаптирован к потребностям вашей фирмы.

На этой стадии могут возникнуть затруднения, поскольку невозможно сравнивать предложения ведущих специалистов фирмы и предложения специалистов охранного предприятия, с которым заключен договор.

Уточнение и проверка формулировки задачи обеспечивают четкое понимание цели, четкий ответ на вопрос: "Чего же мы хотим добиться?"

Какой бы очевидной ни казалась первоначальная формулировка задачи, ее необходимо проверить и уточнить, проведя три обязательные и две желательные операции:

1) определить, какова конечная цель, ради достижения которой поставлена решаемая задача;

2) определить, нельзя ли достичь эту конечную цель "в обход" — решением другой задачи;

3) определить, решение какой задачи, первоначальной или "обходной", дает лучший результат;

4) по возможности оценить количественные показатели результата и их соответствие неизбежно нарастающим требованиям в будущем, когда данное решение будет реализовано;

5) уточнить дополнительные требования, определяемые условиями, в которых предполагается реализация.

В случае необходимости цикл может быть повторен. В итоге получают уточненную формулировку задачи, а иногда и готовое решение, так как может оказаться, что уточненная задача может быть решена готовыми средствами.

Окончательный выбор при принятии решения по обеспечении безопасности и защиты фирмы возможен после проработки проекта защиты объекта.

Рассмотрение плана по организации обороны и защиты объекта от преступных посягательств и при различных чрезвычайных обстоятельствах.

План обороны и защиты объекта разрабатывается для проведения его в действие в следующих случаях:

1) при грабежах и разбойных нападениях, терактах, направленных против фирмы (ведущих специалистов);

2) при нападении на фирму с целью нанесения ущерба или уничтожения производства и материальных ценностей;

3) при возникновении пожара, наводнения, аварии, других чрезвычайных обстоятельствах.

Все выше рассмотренные оценки в решении предпринимателя могут входить в план обороны и защиты объекта.

Как упрощенный вариант рассмотрим на примере все составные части решения, позволяющего обеспечить безопасность и защиту фирмы, ее ведущих сотрудников:

1. Оценка противостоящих сил на рынке услуг (производства) и преступных элементов (групп) в районе (зоне) дислокации фирмы.

2. Оценка своих сил:

- техническое обеспечение защиты фирмы;
- физическое обеспечение защиты;
- качественная характеристика сотрудников СБ;

• выводы из оценки сильных и слабых своих сторон и предложения по их компенсации.

3. Оценка сотрудничающих и взаимодействующих фирм на рынке услуг.

4. Организация взаимодействия постов и порядок их усиления на различных режимах деятельности.

5. Организация связи между постами для обеспечения взаимодействия.

6. Организация взаимодействия с органами МВД.

7. Действия сил и средств службы безопасности при нарушении режимов защиты.

8. Обеспечение охраны ведущих специалистов фирмы, их семей и собственности.

V. ***Оценка противостоящих сил на рынке услуг (производстве) и преступных элементов (групп) в районе (зоне) дислокации фирмы. Организация взаимодействия с органами МВД.***

Задача собирающих и анализирующих информацию заключается в упреждающем выявлении источников внешней угрозы безопасности с тем, чтобы максимально снизить неопределенность стратегического риска.

Предполагается, что такого рода информация должна раскрывать истинные намерения потенциальных и действительных партнеров по отношению к объекту; характеризовать сильные и слабые стороны конкурентов; помогать оказывать влияние на позицию заинтересованных лиц в ходе переговорного процесса; предупреждать о возможном возникновении кризисных ситуаций; облегчать контроль за соблюдением партнерами достигнутых ранее договоренностей; способствовать выявлению несанкционированных каналов утечки конфиденциальной информации о защищенном объекте.

Эффективность координации и взаимодействия во многом зависит от правильности распределения прав и обязанностей между участниками совместных действий, а следовательно, от совершенства правового регулирования, определяющего их компетенцию.

Положительному решению данной проблемы способствовала бы разработка нормативного акта, детально регламентирующего вопросы координации и взаимодействия государственных правоохранительных органов и частных служб безопасности.

Представляется, что данный нормативный акт по содержанию должен состоять как бы из двух частей: первой, определяющей порядок осуществления информационного взаимодействия, т. е. обмена информацией, предоставления одним органом другому сведений, необходимых для реализации стоящих перед ними задач, и второй, где был бы изложен порядок осуществления оперативного взаимодействия (совместного осуществления и согласования планов оперативной работы, проведения спецмероприятий, взаимному использованию сил и средств каждого из подразделений и т. д.).

В первом разделе документа целесообразно обязать руководителей государственных правоохранительных органов своевременно представлять в подразделения безопасности, отвечающие за обеспечение безопасности негосударственных объектов экономики, материалы по следующим вопросам:

1) планы спецслужб и формирований организованной преступности;

2) выявление фактов осведомленности иностранных спецслужб о негосударственных объектах;

3) конкретные лица из числа сотрудников объекта, подозреваемых в проведении противоправной деятельности;

4) вербовочные и иные подходы к сотрудникам объекта, втягивание их в контрабандные, валютно-спекулятивные и иные противоправные сделки;

5) некоторые симптомы возможного проведения иностранными спецорганами дезинформационных мероприятий через официальные и агентурные каналы;

6) поставка заведомо недоброкачественной продукции;

7) факты предпосылок к совершению террористических и диверсионных актов в отношении персонала объекта;

8) попытки захвата материальных и иных ценностей, установления контроля над деятельностью объектов со стороны преступных группировок;

9) проверенные данные в отношении подозрительных связей в криминальной среде отдельных лиц из числа персонала объекта, которые могут быть использованы иностранными спецслужбами и формированиями организованной преступности.

В свою очередь, целесообразно обязать руководителей негосударственных служб безопасности своевременно представлять в государственные правоохранительные органы всю информацию, относящуюся к компетенции данных органов.

Обмен информацией целесообразно предусмотреть как непосредственно между заинтересованными структурами, так и с использованием систем информационного обеспечения.

Во втором разделе предлагаемого нормативного акта целесообразно изложить требования к совместному планированию и согласованному осуществлению оперативных и иных мероприятий на объектах, использованию наличных сил и средств при соблюдении взаимных интересов.

Например, для обеспечения охраны ведущих специалистов фирмы, членов их семей в графическом решении на карте города для организации безопасности и защиты фирмы предусматриваются несколько вариантов маршрутов перевозки ведущих специалистов на автомобиле из дома на работу и обратно. На этих маршрутах предусматриваются контрольные выходы на связь с целью своевременной помощи в случае надобности, места парковки "чистого" автомобиля при уходе от преследования или слежения и другое.

Не рекомендуется на схему решения по всем видам защиты наносить явочные квартиры, их адреса, телефоны, где проводятся переговоры с контрагентами, дилерами и партнерами. Как правило, они должны периодически, незакономерно меняться.

Целесообразно на схеме иметь порядок оповещения сотрудников, сигналы "тревог", кодовые слова для телефонных и радиопереговоров, организацию связи в угрожаемый период и прочее.

После принятия решения и графического исполнения "в мраморе" вся схема складывается до размеров стандартного форматного листа А4 (210 × 297 мм).

После этого схема на местах сгибов разрезается, а с обратной стороны снова склеивается широкой клейкой лептой, что позволяет схему легко складывать и разворачивать, а также хранить в сложенном виде в опечатываемой папке и сейфе дежурного по службе безопасности. Вскрывается схема только при получении условного сигнала тревоги. Все черновые материалы уничтожаются в установленном порядке.

На основании принятого решения составляется расписание действий сотрудников СБ фирмы, которые делятся на тревожные (действия по тревоге) и повседневные.

Сотрудники СБ распределяются по постам с учетом их уровня подготовки, физических качеств и др. Распределение имеет целью обеспечить наиболее полное и эффективное применение всех имеющихся средств, взаимозаменяемость и правильную расстановку с учетом опыта работы.

На основании расписания СБ составляются инструкции на каждый пост, маршрут, объект при различных режимах охраны ("тревога", "угрожаемый период" и "повседневный").

В этих инструкциях подробно излагаются обязанности сотрудников СБ по организации защиты фирмы и ее ведущих сотрудников, порядок применения оружия и спецсредств, использование средств наблюдения и контроля при стихийных бедствиях, а также дополнительные обязанности, определяемые руководителем СБ фирмы.

После составления всех этих документов, их утверждения президентом фирмы проводится отработка организации службы безопасности, как правило, этот срок определяется исходя из реального времени, необходимого для сколачивания и боевого слаживания коллектива, отработки действий каждого поста или объекта, и не превышает 25 дней.

Приведенные рекомендации принятия решения об организации безопасности и защиты фирмы, ее ведущих сотрудников носят скорее эмпирический характер, чем строго научный, так как уни-

кальность и непредсказуемость поведения системы безопасности в конкретных условиях (благодаря наличию у нее активного элемента — человека) и вместе с тем наличие у нее определенных возможностей, определяемых имеющимися ресурсами, способностью изменять свою структуру и формировать варианты поведения, адаптироваться к изменяющимся условиям и наличием стремления к целеобразованию, т. е. формированию целей внутри системы, все же позволяет удовлетворить нужды, потребности и запросы потенциальных потребителей.

3.2. Активные и пассивные средства защиты

Все средства защиты можно разделить на две большие группы: активные и пассивные. К активным можно отнести газовое оружие (аэрозольные устройства и газовые пистолеты, а также газодробовые системы), огнестрельное, а также холодное оружие.

Кроме того, возможно применение электрошоковых и светошоковых устройств, а также светозвуковых шоковых гранат, карманных сирен и тому подобных устройств. Стоит заметить, что любое из активных средств защиты легко превращается в оружие нападения, если обращаться с ним не в соответствии с буквой закона.

3.2.1. Газовое оружие самообороны

Основным назначением газовых устройств самообороны является создание газодымного облака или аэрозольной взвеси в непосредственной близости от нападающего. Состав облака или взвеси определяется моделью заряда и включает в себя физиологически активное вещество раздражающего действия.

При контакте с распыленным веществом у нападающего появляются сильная резь в глазах, мучительное жжение в области носоглотки, задержка дыхания, в некоторых случаях удушье, результатом чего может быть потеря сознания. Это обусловливает успех в

применении таких устройств против вооруженного или превосходящего в физической силе противника. Кроме того, успех применения обеспечивается внезапностью.

Впоследствии у нападающего, оказавшегося в зоне действия физиологически активного вещества, недомоганий не возникает. Время, на которое нападающий "выходит из строя" и становится небоеспособным, зависит от степени концентрации активного вещества в окружающей среде. Концентрация облака или аэрозоля может быть как непереносимой, исключающей всякие действия со стороны нападающего, так и переносимой, имеющей только сдерживающий эффект.

Как правило, переносимая степень концентрации создается на предельной дальности выстрела оружия. В обоих случаях лицо, применившее оружие, имеет достаточно времени для того, чтобы обратиться за помощью, уйти от нападающего или принять меры к его обезвреживанию.

Иногда для того, чтобы вместе с поражением "пометить" нападающего с целью его последующего опознания, применяются боеприпасы, в которых наряду с физиологически активным применяется и нетоксичное красящее вещество.

Самым распространенным химическим веществом, применяемым как в зарубежных, так и в российских аэрозольных и газовых системах, является ортохлорбензальмалонодинтрил, или сокращенно CS. Данное соединение относится к группе отравляющих веществ раздражающего действия и иногда называется слезоточивым газом.

Это твердое, кристаллическое, бесцветное вещество, имеющее специфический вкус, чем-то похожий на перец. Плотность 1,04 г/см^3 (т. е. очень близкая к воде), температура плавления 96 °С.

CS — стойкое соединение, плохо растворимое в спирте и воде, но лучше — в растворителях типа бензола, хлороформа, ацетона. При длительном хранении CS не теряет своих химических свойств.

В газовом оружии вещество CS применяется в аэрозольном состоянии. Выстрелы или распыление могут производится боепри-

пасами взрывного действия или с помощью распыляющих устройств, а также в виде пиротехнических смесей с содержанием действующего реагента до 50%. Выполненное по специальной рецептуре вещество может применяться и в желатиновых капсулах.

Раздражающее действие аэрозоля сохраняется в течение 5–10 мин. Физиологическое действие небольших доз (до 10 мг/м^3) рецептуры, выполненной на основе CS, характеризуется непрекращающимся кашлем, резью в глазах, обильным слезотечением, сдавливанием грудной клетки и затруднением дыхания, выделениями из носа и головокружением.

При воздействии вещества нападающий не способен вести эффективные согласованные действия. Эффект применения определяется не временем воздействия, а степенью концентрации, размерами аэрозольного облака и погодными условиями в момент применения.

В газовом оружии самообороны могут применяться составы на основе CS, которые предназначаются для усиления воздействия путем повышения стойкости аэрозольного облака.

Рецептура CS-1 имеет в своем составе 95% мелкокристаллического вещества CS и 5% макропульверизованного силикагеля. Эта смесь представляет собой мелкодисперсный порошок, имеет низкую плотность и прекрасно распыляется при взрыве. Это обусловило успех применения состава в гранатах и бомбах, а также распылителях воздушного типа.

Смесь CS-2 — это тот же CS-1, но обработанный силиконом, что повышает водоотталкивающие свойства и как следствие — придает высокую сыпучесть. Это позволяет ему долгое время находиться в приземных слоях атмосферы и противостоять метеорологическим воздействиям.

Зарубежные специалисты разработали для газового оружия еще один продукт. Он получил название CR и представляет собой кристаллическое вещество желтого цвета. Вследствие довольно низкой температуры плавления и плотности CR обладает повышенной летучестью, высокой токсичностью и относится к группе сильнодействующих ОВ раздражающего действия.

Вещество в чистом виде хорошо растворяется в спиртах, эфирах, плохо — в воде. Легко взаимодействует с окислителями (перекисью водорода, хлораминами и др.), образуя при этом нетоксичные соединения. Сохраняет стабильность в органических растворах, например таких, как этилен. Все вышеперечисленные свойства говорят о высокой химической активности соединения.

Продукт CR может использоваться в виде тонкодисперсного аэрозоля в газовых системах оружия или входить в состав пиротехнических смесей.

Если контакт с ОВ осуществляется без ингаляционного воздействия, то страдают в основном глаза. Возникает сильная резь, обильное слезотечение и возможна кратковременная потеря зрения. При вдыхании состава возникает раздражение носоглотки, что сопровождается сильным кашлем, чиханием и выделениями из носа.

По степени поражающего воздействия CR более токсичен, чем CS, и достижение того же эффекта требует меньших затрат вещества.

Попадание рецептуры CR на кожу вызывает поражения как при ожогах, причем увлажненное вещество гораздо активнее в этом отношении. Если вещество вовремя удалить с поверхности кожи, то неприятные ощущения исчезнут через 15–30 мин.

В специальных средствах часто применяется вещество CN, или хлорацетофенон.

Данный состав является типичным представителем группы ОВ раздражающего действия. Для токсичного воздействия на органы зрения достаточно мизерной дозы. При больших степенях концентрации CN вызывает не только поражение глаз и слизистых оболочек полости рта и носа, но и раздражение открытых участков тела. В чистом виде состав не имеет цвета и представляет собой мелкокристаллический порошок с приятным запахом цветущей черемухи.

Хлорацетофенон не взаимодействует с водой, очень плохо вступает в реакцию с растворами щелочей. Для дегазации использует-

ся обработка подогретым водно-спиртовым раствором сернистого натрия (NaS).

CN термически стабилен, плавится без разложения и устойчив к детонации. Эти свойства позволяют с успехом использовать вещество в таких специальных средствах, как газовые патроны, аэрозольные упаковки и дымовые шашки (самостоятельно или в смесях с другими составами раздражающего действия).

Все газовое оружие можно разделить на две большие группы:

1. Газовое оружие, использующее боеприпасы пистолетного типа.

2. Устройства, не имеющие в своем составе боеприпасов.

К первой группе можно отнести газовые пистолеты и револьверы, а также устройства дозированного аэрозольного распыления. Ко второй группе относятся газовые баллончики, шашки и тому подобные приспособления.

При покупке газового пистолета или револьвера в магазине необходимо внимательно его осмотреть и убедиться в наличии клейма страны-производителя и испытательного клейма.

Все отечественное гражданское оружие проходит обязательную сертификацию. Как правило, ее проводят предприятия-изготовители или государственная испытательная станция. У них есть свои клейма.

На системах газового оружия, которые производятся в Германии, проставляется аббревиатура "PTB", а под ней число, вписанное в круг. Это означает, что данный пистолет или револьвер невозможно переделать для использования пулевых или дробовых патронов.

Кроме оружия с клеймами Германии и Италии, в России имеет хождение и оружие с клеймами Австрии, Бельгии, Чили, Испании, Финляндии, Франции, Англии, Венгрии, Чехии, Югославии. Все оружие, произведенное в других странах, должно быть сертифицировано в России или в другой из перечисленных стран и получить испытательное клеймо, после чего оно будет иметь хождение на территории России.

Газовые пистолеты

Под газовыми пистолетами и револьверами понимаются системы оружия, которые путем метания веществ слезоточивого раздражающего действия приводят к поражению живой цели.

Создание таких систем, как газовые пистолеты и револьверы, было обусловлено проектировкой и изготовлением патрона, который включает в себя пороховой заряд, химическое вещество и капсюль-воспламенитель, конструктивно объединенные в одну гильзу. При этом патрон является беспулевым, т. е. торец гильзы, где должна находиться пуля, либо закрывается пластмассовым пыжом, либо завальцовывается.

Обязательно при заряжении следует проверять срок годности боеприпасов, просроченные рекомендуется не применять.

Револьвер от пистолета отличает вращающийся барабан, в котором располагаются заряды или патроны, одновременно барабан выполняет функцию блока патронника. В пистолете патроны находятся в специальном магазине, из которого под действием пружины по мере производства выстрелов подаются в патронник ствола.

Внешне газовые пистолеты и револьверы ничем не отличаются от боевых, и это создает дополнительный психологический эффект от вида оружия. Нередко конструкторы берут боевой образец и после небольшой доработки (в основном ствола) получают газовый пистолет или револьвер. Цель данной доработки — исключить применение боевого и дробового патрона.

В настоящее время выпускаются системы калибров 5,6; 6; 7,62; 8; 9 мм, а также 0,315 и 0,45 мм (по стандартам, принятым в США).

В большинстве своем газовое оружие представляет собой достаточно сложные в производстве и эксплуатации конструкции, требующие умелого обращения и тщательного ухода. Газовые пистолеты выпускаются по конструктивным схемам боевых пистолетов с применением материалов, используемых в производстве оружия.

Пистолеты являются автоматическим самозарядным оружием. Ствол имеет цилиндрическую форму и соединяется с рамкой пистолета посредством резьбы или выступов, цепляющихся друг за друга. Внутри гладкого, без нарезов ствола размещается поперечная пластина с отверстием продолговатой формы. Она служит для разрушения пластмассовых пыжей во время стрельбы, а также обеспечивает усиленную отдачу для безотказной работы автоматики управления.

Газовые пистолеты обычно имеют автоматические предохранители, требующие специальной установки в положение для стрельбы и на предохранитель.

Недостатком газового пистолета является возможность перекоса патрона в момент подачи его из магазина в патронник ствола. Происходит это потому, что пистолет является копией боевого и у него снята фаска для облегчения захода пули в патронник.

Никогда не пытайтесь расточить и переделать пистолет газовый под боевой патрон. Материалы, из которого пистолет изготовлен, не годятся для стрельбы пулей. При производстве выстрела пистолет может просто разлететься на куски, в результате чего пострадаете вы.

Многие специалисты-практики утверждают, что в эксплуатации револьвер гораздо надежнее пистолета. Это, разумеется, очень спорный вопрос, но для тех, кто мало тренирован в обращении с оружием, в том числе газовым, посоветуем лучше пользоваться револьвером. Компоновка револьвера выполняется по классической схеме, и практически все модели газового оружия являются копиями боевого.

Ствол револьверов также выполнен без нарезки и имеет стальную перегородку, выполняющую те же функции, что и у пистолета.

Число гнезд для патронов в барабане колеблется от пяти до восьми штук.

Заряжение и перезаряжение револьверов производится вручную, возможно заряжение как боевых моделей — подковообраз-

ными обоймами по три патрона. Для разряжения после отстрела всех патронов используется монтируемый на револьвере шомпол или специальный извлекающий механизм, срабатывающий при откидывании барабана.

Конструктивно револьверы более сложны, чем пистолеты, и их сборка-разборка занимают гораздо больше времени. Ударно-спусковые механизмы газовых револьверов связаны с механизмом вращения барабана, а потому допускается работа в двух режимах: взведением курка вручную и самовзводом.

В настоящее время инженеры-проектировщики разрабатывают новые образцы оружия активной защиты. Основное направление этих работ — повышение эффективности применения. На втором плане стоят способность противостоять нескольким нападающим и комбинирование нескольких видов воздействия в одной системе оружия.

Совершенствуются не только средства применения, но и боеприпасы к ним. Уже созданы, прошли испытания и успешно используются так называемые травматические боеприпасы. Это патроны, в которых вместо физиологически активного вещества используются пластиковые пули или картечь. Испытания показали высокое останавливающее и шоковое действие боеприпасов этого типа.

Среди разрабатываемых комплексов особый интерес представляют бесствольные модели. Они компактны, удобны, при этом не теряют своей эффективности и в них, наряду с травматическими боеприпасами, могут применяться любые другие: с раздражающим ОВ или сигнальные. В России разработан бесствольный комплекс "Оса".

Специальный калибр (18 мм) не позволяет использовать в данной системе охотничьи или боевые патроны. Одновременно заряжается четыре патрона. Система может использоваться с лазерным прицелом. На испытаниях "Оса" показала очень высокую эффективность и надежность. К данной системе самообороны разработаны пять типов боеприпасов, оказывающих разнообразное воздействие на нападающих:

1. Ударно-боевой с травматическим эффектом.

2. Свето-звуковой. Останавливающее действие основано на том, что звук высокой частоты вызывает шок и кратковременную слепоту после яркой вспышки. Эффективная дальность применения — 5 м.

3. Газовый. Классический газовый боеприпас может быть начинен вытяжкой из кайенского перца, что оказывает эффективное останавливающее действие даже на людей с пониженным болевым порогом и животных. Дальность действия — до 5 м.

4. Метящий. Патрон начинен жидкой краской, практически не поддающейся воздействию бытовых растворителей. Дальность действия — 5 м.

5. Сигнальный. Боеприпас снаряжен химическим составом, при сгорании которого образуется звезда зеленого, красного или желтого цвета. Высота подъема составляет 150 м.

Комплекс может быть одновременно заряжен любыми четырьмя видами боеприпасов и производить выстрелы в любой последовательности.

Меры безопасности

Если пользователь будет пренебрегать элементарными правилами обращения с оружием, то любой, даже самый безобидный комплекс может доставить массу неприятностей: перекос боеприпаса, осечка, разрыв канала ствола и т. д. Следствием этого будут травмы.

Чтобы избежать всего этого, следует внимательно изучить инструкцию по обращению с оружием:

1. Не направляйте пистолет (револьвер) в сторону людей, даже если он не заряжен, без необходимости.

2. Не используйте оружие, не изучив приемы и правила стрельбы, устройство, возможные неполадки и способы их устранения.

3. Строго соблюдайте способы и правила технического обслуживания и хранения оружия.

4. Не применяйте боеприпасы, не предназначенные для стрельбы из пистолета (револьвера) данной модели (боевые, самодельные, другого калибра).

5. Следите за чистотой канала ствола, затвора и патронника.

6. После выхода из опасной ситуации или прекращения стрельбы обязательно ставьте оружие на предохранитель.

7. Обслуживание пистолета (револьвера) проводите только на открытом воздухе или в вентилируемом помещении.

8. Избегайте попадания остатков активного вещества на кожу во время чистки оружия.

9. Не переделывайте газовые системы под стрельбу боевыми патронами — в первую очередь пострадаете вы.

10. Учебные стрельбы следует проводить в специально оборудованном помещении — тире с хорошей вентиляцией — или на открытом воздухе, в условиях, исключающих попадание активного вещества на стреляющих.

11. Помните, что при производстве стрельбы против ветра резко возрастает вероятность попадания содержимого патрона на стреляющего.

При работе автоматики пистолета также возможен частичный выброс и попадание содержимого патрона на кожу рук или лица. В этом случае необходима санитарная обработка.

Газовый пистолет, каким бы несерьезным он ни казался, является оружием, имеющим определенные свойства и особенности применения, которые необходимо учитывать. Прежде всего, имея при себе газовый пистолет, не стоит выставлять его напоказ, "красоваться" и демонстрировать без надобности. Все эти действия для тех, кто купил пистолет как игрушку, а не как средство самозащиты. Тем же, кто приобрел пистолет для собственной безопасности, рекомендуем применять его внезапно.

Если вы убедились, что нападающий настроен действительно агрессивно и его намерения вам ясны, дайте противнику сократить дистанцию до метра-полутора и стреляйте на поражение. Не вздумайте производить холостые или предупредительные выстрелы, тем самым вы дадите противнику возможность поменять тактику или принять ответные меры.

Лучшее расстояние для стрельбы на открытом воздухе составляет меньше полуметра. В этом случае исключается воз-

действие ветра или других природных факторов, а также к воздействию газового облака добавляется еще одно — шоковое. Если открывать огонь с расстояния более полутора метров, то стрельба будет малоэффективна, так как на формирование облака окажет влияние ветер, а эффект внезапности будет сведен к нулю.

Если вы сами подверглись нападению человека, вооруженного газовым оружием, и при этом не успели достать пистолет и подготовиться к стрельбе, необходимо в первую очередь оторваться на безопасную дистанцию (около 5 м).

Это легко сделать даже нетренированному человеку, стоит только начать бег первым. Далее нужно достать пистолет, снять его с предохранителя и, резко развернувшись, начать стрельбу, отстреливая заряды один за другим и сокращая дистанцию.

В этой ситуации большую роль играют навыки владения оружием и емкость магазина. Достав пистолет, начинайте стрельбу. Если вы начнете уговаривать противника бросить оружие, то только дадите ему шанс сориентироваться в новой обстановке.

Как поступать в ситуации, если нападающий открыл по вам огонь? Необходимо вести стрельбу патрон за патроном, стараясь сократить дистанцию и "достать" противника. Струя газа, вылетающая из вашего оружия, будет рассеивать струю газа противника.

В этой ситуации необходимо помнить, сколько патронов у вас в магазине, в противном случае, увлекшись, вы будете побеждены. Если вы все-таки попали в облако активного вещества, необходимо принять меры первой обработки, о которых говорилось ранее.

Газовые аэрозольные устройства

Для самозащиты разработаны эффективные средства в виде газовых баллончиков, представляющих собой портативные закрытые емкости цилиндрической формы весом 50–60 г. Газ в них находится под высоким давлением и выбрасывается через сопло специальной конструкции. Нажатие на кнопку или рыча-

жок открывает запорный клапан, и устройство создает газовое облако вокруг нападающего на удалении 1–2 м.

На основе газовых баллончиков созданы и успешно применяются различные устройства специального назначения, выполненные в форме пистолетной рукоятки, авторучки, карманного фонаря, полицейской дубинки и так далее. Все эти приспособления снабжаются механической или электрической системой инициирования, а баллончики с активным веществом заключены в корпуса специальной конструкции.

К классу аэрозольных средств самозащиты можно отнести устройства, применяющие в качестве поражающего элемента капсулу со слезоточивым или любым другим раздражающим газом.

Такие приспособления выполняются в виде короткоствольных пистолетов, а в качестве метательного средства используется, например, баллончик с окисью углерода, который находится в рукоятке. Главным преимуществом таких устройств является увеличение дальности стрельбы до 15 м.

Промежуточное место между аэрозольными устройствами и пистолетами занимает отечественная разработка, получившая название УДАР. Аббревиатура УДАР расшифровывается как "устройство дозированного аэрозольного распыления". Разработчики объединили в этой системе свойства аэрозольного оружия и газовых пистолетов. В результате такого смешения получилось устройство, по своим техническим параметрам не уступающее ни тому, ни другому классу, а иногда и превосходящее их.

С начала 1980-х гг. принцип действия УДАРа был воплощен в системах "Фиалка" и "Жасмин", состоявших на вооружении спецподразделений и зарекомендовавших себя наилучшим образом.

Комплекс УДАР компактен, он гораздо меньше газового пистолета, прост в обращении, не требует чистки, поскольку роль ствола при выстреле играет сама гильза, которая после выстрела автоматически выбрасывается. Вместо спускового крючка применен спусковой рычаг, располагающийся слева для удобства нажатия большим пальцем правой руки.

Риск попадания стреляющего в аэрозольное облако в комплексе сведен к минимуму, причем погодные условия (дождь, снег, ветер) не способны помешать использованию.

Если при выстреле из пистолета до цели, даже находящейся всего в 1,5–2 м, долетает лишь часть активного вещества, то из УДАРа ваш противник гарантированно получит "дозу", достаточную для нейтрализации нападающего на 5–10 мин.

Кроме всех перечисленных у УДАРа есть еще одно преимущество — совершенно безобидный внешний вид, не провоцирующий нападающего на применение боевого оружия, к тому же выстрел производится практически бесшумно. И самое последнее и самое значимое: для приобретения УДАРа не требуется лицензия: пирожидкостный комплекс относится к классу аэрозольных устройств, а их, согласно Федеральному закону от 13 декабря 1996 г. № 150-ФЗ "Об оружии", граждане вправе приобретать свободно.

Стоит предупредить, что при покупке газовых баллончиков следует обращать внимание на сроки годности (год выпуска), страну-производитель и тип активного вещества. Срок годности зависит от степени стабильности активного вещества, которое с течением времени имеет свойство разлагаться.

Название страны-производителя будет свидетельствовать о качестве продукции и степени безопасности устройства. Тип активного вещества для иностранной продукции обозначается аббревиатурой их двух букв. CN, CR, CS — вот три основных химических состава, применяющихся в аэрозолях. Не верьте надписи "нервно-паралитический газ" — это дешевый рекламный трюк, так как отравляющие вещества данного типа являются боевыми и могут применяться только химическими войсками.

Какое оружие выбрать

Разумеется, при выборе средства самообороны необходимо все тщательно взвесить и решить, какое газовое оружие приобрести.

По оценкам многих специалистов, пистолет по многим "боевым" параметрам превосходит револьвер. Он компактный,

скорострельный, многозарядный. Еще один недостаток газовых револьверов состоит в том, что ввиду плохого обжатия барабана газ поступает в зазор между ним и обрезом ствола.

Это приводит к потере эффективности атаки и возможности поражения самого атакующего. Поэтому рекомендуем покупать пистолет. Если же вы все-таки решили купить револьвер, то выбирайте ту модель, в которой зазор между барабаном и обрезом ствола минимальный.

Если вы определились с выбором системы оружия, то встает проблема другого плана: какое оружие лучше — отечественное или импортное? С точки зрения дизайна, западное оружие предпочтительнее. Но отечественное имеет одно решающее преимущество. В отличие от зарубежных систем, изготавливаемых из силумина, наше оружие производится из высококачественной стали. В результате отечественные модели гораздо дешевле и служат дольше.

Немаловажным фактором при выборе оружия становится размер пистолета. Даже человеку, часто встречающему настоящее оружие, ни за что не определить: настоящий перед ним пистолет или газовый, так как большинство моделей являются точными копиями боевых.

В то же время большие пистолеты весят до 1,5 кг и ношение такого оружия, особенно в жаркую погоду, создает массу неудобств. Поэтому совершенно не обязательно покупать пистолет по принципу "большой — значит хороший". Модели Walter PPK или Mauser HSC смогут защитить вас не хуже, а проблем с ношением не возникнет.

Для газового оружия выпускаются патроны и другие типы боеприпасов различного калибра, всего их насчитывается более десяти. Самыми ходовыми из них являются боеприпасы калибром 8 и 9 мм.

Патроны и оружие большого калибра, в данном случае 9-миллиметровые, бьют приблизительно на полметра дальше, чем системы калибром поменьше. Но это не играет какой-либо существенной роли, так как 8-миллиметровые комплексы обеспечивают поражение на удалении 3 м и если прибавить 50 см, то мало что изменится.

Увеличение калибра влечет за собой уменьшение количества патронов в магазине. Например, в модели Reck Miami-92F 9-миллиметровых боеприпасов вмещается 11, а 8-миллиметровых — 18 штук. Пороховой заряд при этом и в том и другом патроне одинаков. Другие калибры патронов не берутся к рассмотрению ввиду их малой мощности и эффективности.

На российском рынке чаще всего встречаются боеприпасы производства Германии и Италии. На упаковке обязательно должно стоять сертифицированное клеймо того изготовителя, где проводились испытания, и штамп, на котором содержится информация о количестве биологически активного вещества в одном боеприпасе.

Для зарубежных патронов оно составляет не более 15%. Патроны с более низким содержанием химического вещества не рекомендуется покупать ввиду их малой эффективности при применении.

Объем химического вещества в них значительно больше, чем в зарубежных, и составляет 25% реагента CS. Недостатком российских боеприпасов специалисты считают низкое качество технологии изготовления. Боеприпасы могут быстро стать негерметичными. Поэтому, как только вы извлечете пистолет из кобуры, начинают слезиться глаза.

Таким образом, из патронов к газовому оружию, представленных на российском рынке, целесообразно покупать импортные боеприпасы калибром 8 мм с содержанием активного вещества не менее 15%, например фирмы Umarex.

Ношение оружия

Для повышения эффективности применения газового оружия важную роль играет время подготовки к стрельбе. Его можно значительно сократить, если носить оружие на полувзводе и с патроном, досланным в патронник.

Кобуру нужно выбирать очень тщательно, учитывая размеры оружия, его марку, способ и место ношения.

Выбор конкретного приспособления для скрытого ношения оружия зависит от размеров и формы оружия, телосложения

владельца. Только самая "откровенная" одежда (купальник, плавки) не позволяет спрятать личное оружие, в остальных случаях всегда можно надежно спрятать пистолет, при этом необходимо учитывать, что извлекаться он должен максимально быстро. Поговорка "Подальше положишь — поближе возьмешь" в данном случае неуместна.

В отношении личного оружия понятие "быстрота" подразумевает не боевую скорострельность, определяемую маркой оружия, а время, затраченное на производство первого выстрела, от момента принятия решения о выстреле до момента вылета струи газа (пули) из ствола.

В течение этого времени происходят извлечение оружия из кобуры, приведение его в готовность к выстрелу (снять с предохранителя, дослать патрон в патронник, если его там не было), подъем оружия на линию выстрела, прицеливание, нажатие на курок, спуск, срабатывание ударно-спускового механизма, выстрел и движение газовой струи по каналу ствола.

Наибольшее количество времени уходит на извлечение оружия. Между тем в кризисной ситуации, при очень короткой дистанции или внезапном появлении противника время извлечения должно составлять не более 0,7 с.

Самым распространенным способом ношения оружия, которым пользуются сотрудники полиции и спецслужб, является подплечная "оперативная" кобура. Им пользуются и обыкновенные граждане, и телохранители, и охранники. Свою роль в распространении такого способа сыграли видеофильмы. Расположение оружия в подплечной кобуре малозаметно под плащом, пиджаком, летней курткой, и траектория движения руки к нему достаточно коротка.

Изготовляется такое снаряжение из двух кольцевых ремней, охватывающих плечи и соединяющихся на лопатках. На одной стороне (справа или слева) крепится кобура, а на другой — своеобразный подсумок для переноски двух запасных магазинов.

Такое приспособление малозаметно, даже если расстегнуть куртку или пиджак. Солидные фирмы производят снаряжение

одной модели разных цветов, что дает возможность подобрать его под цвет рубашки или свитера.

Современные комплекты для ношения оружия могут изготавливаться из синтетики, кожи или быть смешанными. Самыми дешевыми являются синтетические приспособления, выполненные целиком из нейлона или капрона. Их недостатком является то, что искусственные материалы не дают дышать коже и сильно натирают ее.

Более удобны для ношения и доступны по цене комплекты, в которых кобура и несущий ее ремень выполнены из кожи, а остальное снаряжение — из синтетики. Самым дорогим является снаряжение, целиком выполненное из натуральной высококачественной кожи.

Кобуры изготавливают открытыми, с кнопочными застежками или без них. Важно, чтобы застежка легко открывалась пальцем. С внутренней стороны кобуры укреплена упругая прокладка, позволяющая надежно фиксировать пистолет, а также оставляющая кобуру открытой после извлечения оружия с целью быстрого возвращения его назад. Обычное положение пистолета при этом варианте ношения — стволом вниз, рукояткой к корпусу.

Не раз пытались переделать штатную кобуру для пистолета Макарова в "оперативную", но все попытки оказались неудачными. Кобура при малейшем наклоне корпуса выпирала, раскачивалась, а извлечь пистолет из нее можно было только при помощи двух рук. В настоящее время положение изменилось, российский рынок наводнили кобуры из стран ближнего и дальнего зарубежья, а также отечественные образцы.

Например, для ношения револьверов было создано снаряжение с открытой подплечной кобурой, оставляющей рукоятку револьвера открытой. Она может крепиться на корпусе в трех положениях: вертикальном, горизонтальном или наклонном. Для уменьшения времени извлечения подплечные кобуры для револьверов с вертикальным расположением нередко изготавливают с открытой передней частью. После отстегивания фиксатора оружие само вываливается в руку, что позволяет избежать "цепляния" барабаном.

При помещении "длинных" образцов кобуру необходимо смещать вниз, чтобы при извлечении не упереться себе в подмышку. Крупногабаритные модели типа Reck Commander или Reck Miami-92F могут в обычной подплечной кобуре раскачиваться и наносить ощутимые удары по телу. Следует использовать снаряжение с третьим ремешком, фиксирующим кобуру к ремешку брюк, например, как в модели X-3000 "Бьянчи" итальянского производства.

Не слишком большие пистолеты и револьверы, наподобие Walter PPK, рекомендуется носить горизонтально стволом назад: это уменьшает траекторию движения стреляющей руки и несколько сокращает время извлечения. При этом ремни могут быть в форме подтяжек или выполнены в "классическом" варианте.

Пистолет фиксируется за раму при помощи ремешка с липучкой, кнопкой или застежкой-турникетом. Не менее важно и положение запасных магазинов, обычно они располагаются крышкой вниз или вперед, что позволяет существенно сократить время перезаряжения оружия. Магазины в чехлах фиксируются при помощи ремешка на кнопочной застежке.

У снаряжения, в котором применяется способ ношения оружия подмышкой, имеется ряд существенных недостатков. Во-первых, оно не слишком удобно для мужчин с брюшком. Во-вторых, "сбруя" стесняет движение плеч и корпуса, что мешает правильному прицеливанию и сковывает действия в рукопашной схватке. В-третьих, рука, потянувшаяся за пазуху, нередко является предупреждением противнику. Поэтому все чаще личное оружие носят на поясе или в одежде.

На российском рынке очень много миниатюрных, или карманных, моделей. Одним из самых простых вариантов является открытая кобура с упругой прокладкой, которую кладут в карман и фиксируют в нем застежкой.

Несмотря на простоту, приспособление надежно фиксирует оружие и сокращает время извлечения, если, конечно, вы не положили его в глубокий карман брюк или боковой карман пиджака.

Кроме того, оружие в кармане брюк будет характерно выпирать наружу. Для маскировки оружия предлагается приспособление, выполненное в виде рамки и крепящееся к спусковой скобе. Оно придает кобуре прямоугольную форму, и ее можно спутать с каким-либо другим предметом, например, портсигаром.

Самым традиционным способом, особенно у любителей, является ношение пистолета (револьвера) за поясом. Для этого случая также разработаны специальные приспособления.

Открытая кобура без клапана крепится к пистолету при помощи пружинной пластинки, работающей по принципу скрепки для бумаг. Второй вариант — крепление кобуры при помощи петель, такой способ менее гибок, зато более надежен.

Скрытность ношения дополнительно обеспечивается подбором цвета рукоятки. В этом случае к оружию должен прилагаться комплект сменных ручек разных цветов.

Под пиджаком с длинными полами или под курткой до середины бедер будет практически незаметна любая кобура, хорошо прилегающая к телу и подходящая по цвету. Запасные магазины в таком случае переносят в отдельных чехлах на поясе снаружи с другой стороны от кобуры.

Кроме того, иностранные производители, чаще всего из Германии, предлагают поясные кобуры, выполненные в форме ремня. На нем нашито приспособление для крепления оружия — обычно открытая кобура с упругой прокладкой и чехлы для ношения запасных магазинов, чаще всего их два. Такое приспособление очень удобно, так как позволяет укреплять оружие так, как удобно владельцу, быстро снимать и вновь одевать "пояс" с оружием.

Конструкция кобуры может выполнять функции по приведению оружия в готовность к выстрелу: небольшой выступ позволяет снять пистолет с предохранителя, взвести курок и дослать патрон в патронник одной, стреляющей, рукой.

Одни кобуры (системы "Галко") фиксируют оружие за спиной горизонтально, рукояткой вверх, другие — с наклоном в сторону стреляющей руки, что существенно сокращает время движения

оружия и производство первого выстрела. Существует мнение, что противник может заблокировать руку, если вы будете извлекать пистолет из кобуры за спиной. Но если противник находится настолько близко, что блокирует этот способ, то он успешно заблокирует руку и при любом другом.

Стоит отметить лепешкообразную кобуру для скрытого ношения. Конструктивно она представляет собой две наложенные друг на друга половинки. Средняя часть составляет корпус кобуры, а сшитые края — крылья с петлями.

У таких кобур корпус, как правило, формируется под какую-либо определенную модель оружия, и это считается наилучшим решением, так как обеспечивается надежность фиксации пистолета даже без использования закрепляющих ремешков.

Кроме того, лепешкообразная кобура позволяет носить оружие на поясе, под поясом, на подплечном ремне и на бедре, что особенно удобно для женщины.

Для обеспечения скрытого ношения оружия резерва или основного оружия могут использовать кобуры, крепящиеся на голени, под штаниной брюк. Именно так, на широком эластичном ремне крепятся открытые кобуры "Комфорт Локк" и "Лоуренс № 89". Кроме хорошей скрытности, это обеспечивает удобство применения из неудобных положений: за рулем автомобиля, сидя на скамейке и так далее. На голени носят малогабаритное оружие, крупную или среднюю модель будет легко обнаружить и тяжело применить. Для правши кобуру удобнее крепить на левой голени с внутренней стороны. "Револьвер в носке" — штука не слишком удобная, но иногда приходится мириться с отсутствием комфорта, если это обеспечит безопасность.

Все остальные способы крепления — на внутренней стороне бедра, между лопаток (как метательный нож), в рукаве, в шляпе и тому подобных местах — навеяны дешевыми видеофильмами, рассчитанными на не очень разборчивых потребителей.

При быстром извлечении оружия приходится учитывать его форму. У пистолетов наиболее "цепляющимися" частями являют-

ся прицельные приспособления, поэтому образцы с покатым продольным профилем мушки и прикрытыми "ушками" целиком в этом плане предпочтительнее. В револьверах неудобен не укрытый рамкой срез барабана, поэтому для них рекомендуется кобура с открытой передней стенкой.

Для женщин очень удобна модель "Порфолио Плас", которая выполнена в форме дамской сумочки и позволяет носить модели оружия очень крупного калибра. Причем в заднюю поверхность сумочки вмонтирована специальная панель, выполняющая функцию защиты.

Однако постоянно носить оружие при себе вы не сможете, рано или поздно снимете кобуру и уберете оружие. Если это происходит дома, следует учитывать возможность проникновения злоумышленников в квартиру ночью. Держать оружие под подушкой — не лучший способ.

Удобней, когда кобура крепится сбоку у кровати. Открытая, без клапанов и фиксирующих ремешков кобура крепится на конце планки, уложенной под матрацем так, чтобы рукоятка пистолета или револьвера была ближе к руке во время сна. Нащупать и выхватить оружие из такой кобуры легко даже спросонок, а дополнительное удобство в ориентировании в обстановке обеспечит фонарик, закрепленный рядом с оружием.

Крепить оружие при помощи клейкой ленты к дверному косяку или снизу столешницы не следует.

Таким образом, мы рекомендуем выбирать кобуру только после того, как вы определитесь с моделью оружия, которую хотите приобрести. Если вы выбрали крупногабаритную модель типа копий боевых пистолетов 45 калибра, то наилучшим способом ношения будет подмышечная кобура, опущенная чуть ниже и оборудованная третьим ремешком для крепления к поясу.

Если вы предпочли модели среднего размера типа Walter PPK, некоторые модели беретты и кольта, то можно использовать как кобуру с вертикальным ношением оружия, так и лепешкообразные кобуры с наклонным расположением рукоятки.

Малогабаритные модели удобно носить в кобуре, размещенной на ремне, на голени или в кармане.

Выбор кобуры является делом сугубо индивидуальным, и при подборе ее в магазине вам следует проконсультироваться с продавцом, примерить снаряжение на себя. Предпочтение при выборе приспособления следует отдать тому, которое изготовлено из натуральных материалов, т. е. из кожи. Избегайте некачественного товара, который могут подсунуть вам на рынке.

3.2.2. Помповое оружие

Единственным огнестрельным оружием, которое может применяться в целях самообороны, является гладкоствольное.

Специалисты считают, что именно эта длина позволяет спрятать оружие под верхней одеждой, без риска быть замеченным в ношении. Таким образом, в категорию запрещенных попадают все пистолеты-пулеметы типа "Клин", "Бизон", "Узи" и т. д., а также автоматы АКС, АКСУ и аналогичные им иностранные образцы.

Отсюда следует, что самым удобным и доступным (при оформлении необходимых документов) является гладкоствольное ружье. Одно из первых мест по популярности в "цивильной" среде занимает одноствольное ружье с трубчатым подствольным магазином перезарядки, функционирующим от возвратно-поступательного движения цевья.

Однако по мере реального распространения этого оружия стало очевидным, что его популярность в СНГ зиждилась прежде всего на слухах о нем и на кадрах из боевиков.

Три основные проблемы снижают в условиях СНГ объективно высокую пригодность помповых ружей для самообороны — отсутствие самого оружия, патронов к нему и навыка обращения с ним.

Среди современных моделей наибольшее признание получили Remington-870 и 1100, Mossberg-500, Winchester-1200 и 1300.

В России такое оружие приобрести практически невозможно. В лучшем случае вам предложат бразильские лицензионные изде-

лия, а также ружья, произведенные на Филиппинах и в Китае. Поскольку в условиях России фирменный знак не может служить гарантией качества, выбор оружия должен осуществляться посредством осмотров и тестов.

Особое внимание стоит обратить на механизм перезарядки, так как в случае его отказа многозарядное ружье становится однозарядным. Здесь следует заострить внимание на количестве штанг, передающих усилия от цевья на затвор.

Предпочтительней модели с двумя штангами. Если штанга одна, более надежной будет конструкция с жестко закрепленным цевьем. Чем больше цевье проворачивается вокруг магазина, тем больше накрутка на штангу, тем меньше ресурс ружья. Кроме того, перегиб штанги приводит к неизвлечению гильзы или недосылу патрона.

Ружья, имеющие только один вырез, предназначенный и для заряжания, и для экстрагирования гильзы, хороши на охоте, так как из них гильзы выпадают прямо под ноги. Для боевых ружей характерны два выреза: один для заряжания, второй для выбрасывания гильзы.

Даже идеально прямолинейное движение цевья не гарантирует безупречного выбрасывания гильзы и досылания патрона. Это связано с несовпадением допуска иностранных патронников и отечественных боеприпасов. В иностранных ружьях лучше использовать калиберные импортные боеприпасы заводского снаряжения. Только они позволяют реализовать заложенный в оружии потенциал мощности.

Техника стрельбы из магазинных ружей требует ряда стойких навыков, выработать и закрепить которые можно лишь с помощью систематических тренировок. Стоит запомнить, что рабочий ход цевья составляет около 10 см и движение вперед необходимо выполнять так же активно, как и движение назад.

В противном случае затвор будет закрыт не до конца, спусковой крючок блокирован и выстрела не произойдет. При пользовании помповыми ружьями необходимо выработать рефлекс "выстрелил — передернул", т. е. досылать патрон в патронник следует не перед новым выстрелом, а после предыдущего.

Помповые ружья имеют простую конструкцию, рассчитанную на применение мускульной силы. Показателем правильной перезарядки служит экстракция стреляной гильзы, которая должна выбрасываться и лететь далеко. При медленном открывании затвора зацеп выбрасывателя может не сработать и не захватить закраину гильзы.

По вышеперечисленным причинам специалисты считают, что для гражданского пользователя больше подходит другой тип оружия. Их два: самозарядное и двуствольное. Лучшими моделями, пригодными для использования в целях самообороны, считаются российское ружье МЦ21-12, а также иностранные Browning Mod.-5, Browning B-200 .

Стоит заметить, что в целях самообороны оружие калибров 20, 32, 410 вряд ли будет эффективным, так как такие системы требуют прицельного ведения стрельбы по уязвимым местам, что не всегда возможно в сложной ситуации.

Оружие самообороны должно компенсировать мощностью огрехи прицеливания.

Классическим в этом отношении являются двуствольные ружья 12 и 16 калибра.

Среди неспециалистов нарекание вызывает "немногозарядность" двустволок. В жизни необходимым бывает лишь "третий" выстрел. Ратуя за пяти-восьмизарядные магазины, как-то упускают из виду, что, если на вас напали даже трое вооруженных людей, шансы выжить равны нулю. Поразить удастся только одного-двоих, а двустволка именно для того и предназначена.

Преимущество в скорострельности обеспечивается за счет лучшего баланса: отсутствие подвижных частей автоматики и большая масса обеих стволов. Двуствольное ружье отличается безотказностью, так как его второй ствол служит достаточной гарантией.

Двуствольное внешнекурковое ружье производства Тульского оружейного завода во всех моделях, от ТОЗ-Б до ТОЗ-80, является одним из лучших российских ружей и вполне пригодно для самообороны.

3.2.3. Холодное оружие

Это оружие, предназначенное для поражения цели при помощи мускульной силы человека при непосредственном контакте с объектом поражения.

Подразделяется на ударное, колющее и рубящее, а также сочетающее несколько из перечисленных признаков (например, коляще-рубящее, ударно-рубящее), один из которых является превалирующим.

Нож тоже является средством защиты деловых людей, рискующих в силу своей деятельности оказаться в экстремальной ситуации. Именно здесь нож — инструмент выживания, спасения жизни. Он обязан верно служить хозяину в любое время.

В настоящее время на рынке присутствует огромное количество ножей различных моделей и различного назначения.

Puma ("Пума") — старинная немецкая фирма, продукция которой предназначена любителям острых клинков. На всех ножах Puma есть пометка "ручная работа". Долговечность и хорошие режущие свойства ножа зависят от твердости клинка. Именно поэтому тщательнейшим образом подбираются марки сталей, различные свойства которых позволят каждому ножу соответствовать своему прямому назначению. Для рукояток ножей Puma использует натуральные материалы: олений рог, малахит или дерево твердых пород. В последнее время Puma стала использовать лучшие композитные материалы.

Собранный нож переходит в следующие руки: для оформления граней рукоятки, наведения легкой или глянцевой полировки (в зависимости от модели) с помощью точильного круга, обтянутого кожей или войлоком, покрытым мелкой наждачкой. Последний мазок — это заточки на точильном кругу с очень мелким зерном. Благодаря такой технологии каждый нож Puma уникален. Многие клинки служат своим владельцам десятилетиями.

Одна из самых известных серий складных ножей — Jagdmesser.

Это высококачественные ножи с количеством инструментов от одного до пяти. Щечки ручки ножа сделаны из оленьего

рога, сверху на ручке имеется латунное оголовье. Ножи с одним лезвием, а также с лезвием и пилкой выпускаются с рукоятками из дерева.

Среди нескладных охотничьих ножей выделяется знаменитая модель White Hunter. Нож сделан в чисто германском стиле, который прельщает легким налетом старины и ножнами, дополняющими это впечатление. Он имел всемирный успех и послужил образцом для многочисленных подражаний.

Самая популярная в мире серия складных ножей Puma — серия "четыре звезды". Это 15 моделей с различными длинами лезвий (6 и 8 см) и материалами для рукоятей: от оленьего рога до нержавеющей стали. С 1970 г. Puma выпускает коллекционные ножи этой серии с рукоятками из драгоцегтых камней (малахит, яшма, оникс и т. д.).

Красивые ножи традиционной формы серии Buck широко известны в Европе. Модели Deer Hunter, Game Warden, Lord имеют двойное латунное оголовье, рукоятки из дерева и запатентованной марки резины Kraton.

В серии Protec представлены ножи с лезвием из металлокерамики — легкие, прочные и нержавеющие.

Puma выпускает несколько моделей цельнометаллических ножей, которые также имеют своих поклонников. Каждый такой нож собран на винтах, что делает его полностью разборным.

Знаменитая уникальная модель Waagemesser с рукоятью из нержавеющей стали, заканчивающейся шариком, создающим противовес, и зазубренным лезвием предназначена для рыбаков. Нож позволяет взвешивать пойманную рыбу весом от 250 до 2500 г.

Puma предлагает также престижные коллекционные модели полностью ручной сборки. Каждый такой нож выпускается ограниченной серией (до 300 шт.), имеет свой серийный номер и сертификат качества. Лезвия сделаны из самых лучших материалов: стали ATS-34, дамасской стали, титанового сплава. Это достаточно дорогостоящие, но великолепные вещи.

Solingen — известный центр ножевого производства, но не единственный в Европе. Например, во Франции таким же центром

является Тьер, в Англии — Шеффилд. Solingen — это зарегистрированный торговый знак, когда он применяется к ножу. Только на ноже, все операции по производству и отделке которого выполнены непосредственно в г. Золингене, может быть такая надпись. Покупателям ножей этой фирмы следует знать, что в Китае есть город с названием Solingen, который также использует свое имя на ножах местного производства. На настоящем немецком ноже помимо названия города (Solingen) и страны (Germany) должно стоять и название фирмы.

Современные складные ножи можно условно разделить на две различные категории: нож с одним лезвием и мультиинструментальный нож (мульти-тул), в котором кроме самого лезвия присутствуют и дополнительные инструменты.

Американская фирма Gerber производит широкую номенклатуру складных ножей и мультиинструментальных средств. Ножи серии Gator — одни из лучших складных ножей на рынке. Мульти-тулы имеют много сторонников. В сравнительно небольшом корпусе можно поместить множество самых разных инструментов: плоскогубцы, кусачки, отвертки, открывалки, ножницы, штопор, ножовка и др. Выпускаемые фирмой Gerber с 1997 г. мульти-тулы серии Multi-Plier 600 считаются одними из самых популярных в мире.

Клинок. Профиль клинка на всех моделях — "сабельный", пятигранный. Толщина идеальна: не слишком большая (чтобы мешать при работе) и не слишком маленькая. Формы клинков также отличаются разнообразием.

Масса и баланс. Нож легкий, баланс можно подобрать по руке — даже на одной модели благодаря ручной сборке возможны небольшие вариации на любой вкус.

Рукоятка. Она должна быть достаточно прочной, удобно лежать в руке, не выскальзывать и не размокать, и, кроме того, быть "теплой", не холодить руку. Поэтому в качестве материала для ручки ножа используются береста, кап, древесина европейского и американского ореха, палисандр и другие экзотические породы. Все рукоятки проходят тройную пропитку особыми составами на натуральной основе, что делает их абсолютно не восприимчивыми к влаге.

Гарда. На ножах "Южный крест" нет гарды, т. е. выступа на рукоятке ножа, не позволяющего руке соскользнуть на лезвие. Дело в том, что отсутствие гарды и стало главным признаком, позволившим отнести эти ножи к хозяйственно-бытовым, а не к холодному оружию. Наличие гарды (согласно нормативной документации — более 5 мм) однозначно относит ножи к разряду холодного оружия, что подразумевает совершенно другой порядок их покупки, хранения, ношения и, естественно, цены.

Ножны. Ножны "Южного креста" отличает прежде всего то, что сделаны они из качественной, хорошо окрашенной кожи с заделанной линией среза, аккуратной прошивкой лавсановой нитью, прочной и не подверженной гниению, имеют кольцо на наконечнике и клепку возле устья, возможность разных способов ношения, в том числе даже горизонтального. Нож плотно сидит в ножнах и не болтается. В то же время он легко извлекается без лишних усилий.

Дизайн. Все ножи выдержаны в строгом стиле, имеют свою индивидуальность и поэтому легко узнаваемы. Характерны великолепная полировка клинка, тщательная отделка, продуманная эргономика, сочетающиеся материалы.

Легальность ношения. Многие государства законодательно регулируют действия граждан, владеющих тем, что государство считает оружием. Так, например, в более-менее либеральных к оружию США за последние десятилетия было последовательно запрещено ношение в черте города нескладных ножей с длиной клинка более 4 дюймов, автоматических, гравитационных и инерционных. В некоторых штатах закон еще более строг.

В Великобритании ношение ножей с фиксатором клинка запрещено, существуют жесткие ограничения по его длине для ножей без фиксатора.

Российское законодательство не является исключением. Практика показывает, что практически любой нож, изъятый при обыске или досмотре, при определенных обстоятельствах может быть признан холодным оружием со всеми вытекающими для его владельца последствиями. Это не распространяется только на модели, прошедшие экспертизу.

Основные признаки холодного оружия.

1. Твердость клинка — более 40 единиц по Роквеллу. Метод измерения твердости по Роквеллу заключается в том, что под определенным усилием в поверхность материала запрессовывается стальной шарик. Затем под микроскопом измеряют глубину образовавшейся воронки. Чем она глубже, тем мягче материал.

2. Длина клинка — более 90 мм.

3. Толщина клинка — более 2,5 мм.

4. Наличие гарды (упора для руки).

5. Жесткость клинка (отсутствие остаточных деформаций после приложения определенного усилия на изгиб).

6. Возможность быстрого приведения в рабочее положение (кнопочные, инерционные, гравитационные ножи).

Складные ножи должны хорошо закрываться. Наиболее удобна деревянная рукоятка.

Ножны должны иметь надежную застежку и петлю для ношения на поясе.

Нож всегда должен быть заточен и готов к использованию. Его не следует метать или каким-то иным образом использовать не по назначению.

Храните нож в чистоте, покрыв лезвие тонким слоем смазки. Когда нож не используется, он должен находиться в ножнах.

3.2.4. Бронежилеты

Бронежилеты относятся к средствам пассивной защиты.

Число фирм, производящих и продающих шлемы, бронежилеты и другие средства индивидуальной защиты, все время растет. Сегодня в СНГ более 35 фирм так или иначе осваивают эту новую для себя продукцию.

Кроме того, российский рынок заполняется сравнительно дешевой защитной продукцией из Китая, Кореи, Сингапура, Израиля. Однако проверки этих бронежилетов, проводимые испытательно-сертификационным центром Научно-исследовательского института стали — главного отечественного разработчика подобной продукции — показывают, что около половины из них бронежилетами на самом деле не являются.

Чаще всего продукцией, не получающей сертификата качества, являются бронежилеты, произведенные в странах Юго-Восточной Азии и некоторые модели из стран бывшего социалистического лагеря. Бронежилеты, произведенные в Израиле, зарекомендовали себя неплохо, имевшиеся недостатки были исправлены в более новых моделях (ликвидированы зазоры на боку, в местах застегивания, более защищено горло, мягкая подкладка выполнена из пористого материала).

Бронежилет остается самым ходовым товаром и на армейском "черном" рынке. Продают не только старые, списанные экземпляры (можно только предположить последствия использования такого товара в реальных условиях), но и совершенно новые.

Но многие покупатели совершенно не учитывают, что армейский жилет имеет надежное противопульное бронирование только спереди. Сзади же, как правило, имеется только противоосколочная защита, которая не спасет от выстрела даже из короткоствольных моделей оружия, имеющих низкий убойный эффект.

Среди отечественных изделий армейские специалисты выделяют прежде всего 6Б5 и 6Б10 — модернизованные версии знаменитого жилета 6Б2, использовавшегося в Афганистане. Титановые пластины на них перекрывают друг друга и крепятся на высокопрочном пакете из 30 слоев ткани СВМ. Этот российский вариант американского кевлара шьется из нитей, которые, работая на растяжение, гасят кинетическую энергию пули.

Эти модели бронежилетов прошли боевое крещение в Нагорном Карабахе, в зоне грузино-абхазского конфликта и других горячих точках. Следует сказать, что кевлар не защищает от колющих ударов ножом, заточенной отверткой или шилом. Модели 6Б5 и 6Б10 выдерживают выстрелы из автоматов "Узи", АКСУ и других моделей короткоствольного автоматического оружия. Отличаются они только степенью защиты (Б5 или Б10) и соответственно массой.

Еще большей прочностью отличается костюм "Воин", изготавливаемый для бойцов подразделений специального назначения. Он

способен выдержать очередь из АКСУ или АКМ в упор, близкие разрывы гранат. Как правило, в комплект к костюму входит шлем со стеклом "триплекс", способный выдерживать выстрелы из вышеперечисленных моделей оружия.

Аналогом нашего шлема является шлем, производимый австрийской фирмой *TIG* и состоящий на вооружении у подразделения "Альфа".

На основе бронежилета скрытого ношения (БЖСН) для армейских нужд и для продажи в розницу разработан бронекомплект "Ангар" — противопульный костюм с карманами для снаряжения или дополнительного бронирования.

Разновидность БЖСН — защитная куртка БЖК массой 12 кг. В ее состав, кроме БЖСН, входит кокетка с бронеэлементами, рукава со стальными пластинами и стойка-воротник из гасящей энергию пули ткани ТВСМ-ДЖ. Естественно, БЖК защищает не только туловище, но и плечи, руки и шею.

Еще одна модель, изготавливаемая НИИ Стали, — бронежилет "Прохор", обеспечивающий защиту от холодного оружия. Он значительно легче БЖСН, но вполне надежно защищает и предохраняет от ударов ножом, финкой, заточкой, нунчаками.

Об экипировке полиции и служб охраны надо говорить отдельно. В настоящее время все модели, состоящие на вооружении у спецслужб, доступны любому, у кого появилась нужда в их использовании. Выделяют четыре так называемых "базовых" изделия.

Бронежилет скрытого ношения весит 4 кг и выдерживает удары пуль израильского автомата "Узи" и винтовки М-16, наших АКМ и АКСУ.

В карманы грудной и спинной секций жилета вставлены перекрывающие друг друга и выполненные с изгибом (для лучшего прилегания) бронепластины. Секции соединяются ремнями, под жилет надевается "мягкая" броня — пористые термостойкие блоки, выполняющие сразу две функции: гашение удара и снижение температуры защитной одежды.

Есть и облегченный вариант с пластинами толщиной 3 мм. Этот бронежилет прикроет от выстрелов из пистолета или ре-

вольвера, в ряде случаев защитит и от автоматной очереди, но его предел — пуля, летящая со скоростью выше 440 м/с. Поэтому очередь в упор он не выдержит.

Бронепластины к бронежилетам изготавливаются из титановых сплавов или высокопрочных легированных сортов стали, имеющих большой коэффициент вязкости.

По статистическим оценкам английских криминалистов, более 80% всех убийств совершается холодным оружием. Это поставило перед специалистами задачу о создании бронежилетов для защиты от холодного оружия. Пока это удалось нашим инженерам, а также специалистам из Швеции.

Лучшие достижения НИИ Стали вобрал в себя противопульный представительский комплект "Визит" — с виду обычный костюм-тройка, в котором заложены четыре степени защиты. Ближе к телу — бронемайка из мягких гасящих материалов. Затем жилетка с титановыми пластинами, весьма экзотический бронегалстук и, наконец, пиджак.

"Визит" выдерживает очереди из "Узи" и другого автоматического оружия с расстояния 5–7 м, предохраняет от осколков гранаты, если эпицентр взрыва находится на расстоянии 5 м.

Совсем недавно были рассекречены изделия "Папка", "Планшет" и "Одеяло". Эта продукция состояла на оснащении службы охраны российского президента.

"Папка" весит 8 кг и может открываться за одну секунду, образуя противопульную мягкую броню площадью около 1 кв. м.

"Планшет" побольше и потяжелее. Основное его отличие от "Папки" — узкая бойница в верхней части, позволяющая отстреливаться из пистолета.

"Одеялом" пользуются антитеррористические группы. 27-килограммовое бронеполотно набрасывают на подозрительные объекты, которые могут содержать взрывные устройства. В развернутом виде "Одеяло" может защитить сразу трех человек.

Следует сказать, что бронежилеты, защищая от смертельной опасности огнестрельного ранения, не могут предотвратить такие травмы, как гематомы, переломы ребер, а также повреждения внутренних органов.

При выборе средства защиты в первую очередь необходимо определиться, от какой опасности, вам грозящей, нужно защищаться. Осуществляя выбор, обязательно удостоверьтесь, что бронежилет или другое средство защиты имеет сертификат, выданный каким-либо государственным учреждением, лучше — уже упоминавшимся НИИ Стали. Естественно, узнайте, какую степень (класс) защиты обеспечивает изделие. Всего их бывает пять, но, как правило, степени, имеющие мощное бронирование, простому человеку просто не потребуются.

Как правило, гражданские изделия имеют внешнюю оболочку из черного материала, бронежилеты, производимые для вооруженных сил, окрашены в камуфлирующий цвет. Позаботьтесь о том, чтобы изделие подходило вам по размеру и при одевании сидело плотно, не ерзало и не создавало дискомфорт. И, конечно, ваши желания должны совпадать с вашими возможностями.

3.2.5. Сигнальные устройства

Кроме бронежилетов, к пассивным средствам самозащиты относятся различные устройства, выдающие сигнал о том, что на вас совершено нападение. Устройства этого класса недороги, просты в обращении, что позволяет пользоваться ими даже ребенку.

Карманные сирены. Представляют собой малогабаритные устройства, включающие в себя источник питания и пьезоэлектрическую или электронную сирену. При нападении на вас стоит нажать кнопку, и раздастся высокочастотный звук (визг), который шокирует нападающего. В это время вы сможете предпринять дополнительные меры по защите.

Радиомаячки. Эти устройства маскируют под предметы обихода и носят при себе. Примером может служить радиомаяк, выполненный в форме пуговицы и пришитый к одежде. В случае нападения на вас (возможно, с целью похищения) маяк выдаст тревожный сигнал, фиксируемый приемной стороной, находящейся, например, в агентстве по охране или органах МВД. Недостатком данной системы являются малый радиус действия и довольно высокая стоимость.

3.2.6. Электрошоковые устройства

Электрошоковое устройство — это оружие, применяемое на короткой дистанции, чаще в ближнем бою, для нанесения повреждений или выведения из строя нападающего воздействием на него короткого импульса тока высокого напряжения.

Конструкция электрошоковых устройств очень проста: аккумуляторная батарея, накопитель (боевой конденсатор) и контакты, посредством которых осуществляется разряд. Аккумулятор устанавливается в тех устройствах, которые позволяют осуществить от 5 до 25 разрядов. Существуют также одноразовые шокеры, которые заряжаются от промышленной сети.

Физиологическое воздействие шокеров обусловлено судорожным сокращением мышц, а также внутренних органов под воздействием тока высокого напряжения (до 10 тысяч вольт). Несмертельное воздействие обеспечивается коротким периодом действия и малой силой тока в таких устройствах. Для людей с больным сердцем поражение электрошоком может быть смертельным.

Шокеры изготавливаются любой формы и габаритов. Есть малогабаритные модели, помещающиеся в кармане, и более крупные, предназначенные для специальных подразделений. Малогабаритные используются в качестве оружия самообороны и воздействуют только при непосредственном контакте с нападающим.

Модели для спецподразделений могут наносить поражение на расстоянии до 10 м посредством выстреливаемых контактов, соединенных с устройством тонкой проволокой. Гражданские варианты электрошоковых приборов способны обеспечить от 1 до 10 разрядов, профессиональные модели позволяют делать до 25 разрядов.

В сложной ситуации электрошоковое устройство очень удобно, так как внешне прибор выглядит безобидно и не вызывает настороженности со стороны нападающего.

Стандартным способом применения шокеров является следующий: вы даете атакующему возможность приблизиться к вам на максимально короткую дистанцию, а затем прибором, зажатым в

правой или левой руке, наносите короткий тычок в открытые участки тела. Устройства обеспечивают воздействие и через одежду, но лучше непосредственный контакт.

Для покупки этого вида защитных средств не требуется специального разрешения или оформления лицензии в органах внутренних дел. Такие устройства рекомендуются женщинам, так как шокеры просты в обращении, не требуют специальных навыков для овладения приемами пользования, имеют привлекательный внешний вид и легко помещаются в кармане или сумочке.

3.2.7. Светоимпульсные устройства

К оружию самообороны светоимпульсного типа относятся устройства, воздействующие на злоумышленника яркой вспышкой белого света, что вызывает поражение органов зрения: кратковременную слепоту, ожоги сетчатки. Приборы этого типа максимально эффективны при использовании их в темноте или сумерках. На свету, особенно ярком солнечном, эффект не будет таким шокирующим.

По своей конструкции светоимпульсные устройства очень похожи на электрошоковые приборы. Они включают в себя элемент питания, накопитель электричества (конденсатор) и импульсную лампу, чаще всего галогенового типа. Аккумулятор обеспечивает до ста вспышек лампы без подзарядки. Устройства безаккумуляторного типа, в которых конденсатор заряжается напрямую от сети, обеспечивают только одну вспышку, но очень яркую.

Достоинствами такого типа устройства являются: во-первых, очень быстрый поражающий эффект; во-вторых, применение на дистанции до 5 м (т. е. исключение близкого контакта); в-третьих, безобидный внешний вид, что не вызывает у нападающего желания достать оружие (если таковое у него имеется).

Единственным недостатком данного типа устройств может быть возможное повреждение стекла и лампы прибора, что приведет к неисправности оружия.

Применять светоимпульсные устройства лучше всего с дистанции 1–3 м, неожиданно, чтобы злоумышленник не успел прикрыть глаза руками или шапкой. Прибор необходимо включить за 1–2 мин до его использования, так как для зарядки конденсатора необходимо какое-то время. Лучше всего светоимпульсное устройство носить в кармане пальто или куртки, так как из сумки достать прибор за короткий промежуток времени невозможно, а преступник будет действовать быстро.

Светоимпульсные устройства очень просты в эксплуатации и надежны, даже ребенок способен воспользоваться ими при необходимости. Кроме того, приобретение приборов не требует специального разрешения или оформления лицензии, что делает их доступными для простых граждан.

4. БЕЗОПАСНОСТЬ ЗАРУБЕЖНОЙ ПОЕЗДКИ

4.1. Безопасность деловой поездки

4.1.1. Общие правила безопасности

Деловые люди, посещающие регионы высокого риска, должны обратить внимание на следующее. Хотя уровень риска от страны к стране меняется, теракты в разных государствах продемонстрировали, что терроризм и преступность могут настигнуть везде. И помните: простое хищение вашего паспорта может сорвать деловую встречу.

Сконцентрируйтесь на подготовке к своей поездке.

• Получите обзор ситуации об уровне безопасности в стране назначения. Ваша фирма должна обеспечить вас свежей информацией, а не тем, что произошло во время последнего визита кого-то из сотрудников в эту страну. Ситуация меняется быстро, и ваша информация верна для текущей недели.

• Предусмотрите время на необходимые прививки для въезда в страну. Можно начинать готовиться за несколько недель.

• Узнайте план действий вашей фирмы на случай непредвиденных обстоятельств. Вам нужна эта информация, если с вами что-то произойдет, или на случай форсмажорной ситуации за рубежом.

• Если вы не уверены, что ваша фирма способна помочь вам в чрезвычайной ситуации, разработайте свой собственный план и поставьте в известность свою семью и фирму. Оставьте семье и друзьям список контактных адресов и телефонов.

• При обострении внутренней ситуации правительства западных стран принимают меры к эвакуации своих граждан. Если в стра-

не имеется большая колония деловых людей или бывших соотечественников, правительство может организовать эвакуацию с привлечением вооруженных сил. Поэтому, если вы занимаетесь бизнесом в неспокойной стране, вступите в контакт со своим посольством или консульством. Они должны знать, что вы находитесь в стране, и в случае необходимости помочь вам. Сообщите им, где вы остановились, цель вашего визита и даты прибытия и отъезда. Дайте им номер вашего контактного телефона.

• Найдите больницу или клинику по соседству с местом, где вы остановились, и узнайте, как туда добраться, какую помощь они могут оказать и когда работают.

• Сообщайте вашей фирме на родине о всех своих перемещениях и изменениях планов. Составьте перед поездкой график контактов с офисом. Если вы будете звонить, скажем, в 9 часов утра, пусть это будет короткий звонок, чтобы показать, что связь работает и что у вас все в порядке. Можно сделать главный звонок в 17 часов, чтобы сообщить, как прошел день, включая результаты деловых встреч. Во время каждого звонка в офис сообщайте, где вы находитесь, как долго намереваетесь там оставаться и когда вернетесь в отель. Если вы пропустите один из этих звонков, и с вами не будет контакта в течение 12 часов, это насторожит ваших коллег. Если вы пропустите два звонка, это встревожит коллег в вашем офисе, и они объявят план розыска.

• Не давайте кому попало свою визитную карточку.

• Находясь в незнакомом городе, всегда имейте при себе карту этого города. Полезно изучить маршрут по карте, возможно, с помощью персонала отеля, чтобы узнать, от каких районов нужно держаться подальше.

• Не сообщайте всем подряд, где вы остановились. Если вы живете в отеле, не давайте номер своей комнаты и номер телефона. Чем меньше людей знает, чем вы занимаетесь, тем безопаснее для вас.

• Отвечая на звонок, не называйте себя. Если вы не знаете звонящего, вежливо положите трубку. Не сообщайте ничего о себе или

о коллегах по телефону отеля. Остерегайтесь звонков портье, они могут быть ложными.

• Если вы сами ведете машину или едете на такси на важную утреннюю деловую встречу, узнайте ситуацию на дорогах. Закажите такси накануне, сказав, когда вы должны быть на месте. Вам скажут, когда надо выехать.

• Многие деловые люди имеют при себе в поездке важные документы и значительную сумму наличными. Не кладите их в карманы или в футляр ноутбука. Кошелек через плечо, который можно носить под одеждой, вмещает значительное количество денег и бумаг. Выберите оттенок под цвет вашей кожи. Яркий голубой или красный цвет может просвечивать сквозь светлую рубашку. Избегайте сумок на ремнях, которые легко срезать.

• Узнайте, не планируется ли во время вашего пребывания в городе каких-либо манифестаций. Во время этих событий лучше оставаться в отеле. Местные жители могут дать информацию о характере мероприятия. Следуйте их рекомендациям и узнайте, где наиболее опасное место.

• Если вы знаете местный язык, то, находясь в стране, читайте газеты и слушайте радио, чтобы быть в курсе событий. Если на улицах раздают листовки или стены разрисованы граффити, возьмите это себе на заметку. Это может означать начало кампании гражданских акций или предупреждать, что в стране неспокойно.

4.1.2. Чрезвычайные ситуации

Куда бы вы ни ехали, вы должны быть готовы к возможности ***пожара*** в зданиях, которые вы будете посещать.

• Познакомьтесь с системой тревожной сигнализации и процедурой эвакуации, даже если вам предстоит только деловая встреча. Если вы должны провести в здании некоторое время, пройдите аварийным маршрутом, что облегчит вам задачу в чрезвычайной ситуации. Маршруты эвакуации обычно вывешены на лестничных площадках и в вестибюлях крупных офисных зданий.

• Если включилась пожарная сирена, сохраняйте самообладание, не паникуйте, так как это передается другим и приводит к дальнейшему хаосу. Если вы обнаружите источник огня и попытаетесь сами его потушить, помните, что это допустимо, только если очаг возгорания невелик и вы знаете, где находятся противопожарные средства.

• Большинство офисных зданий имеют начальников пожарной команды, ответственных за безопасную эвакуацию.

• При эвакуации быстро покиньте здание через ближайший аварийный выход. Помните, что надо закрыть за собой дверь. Не берите тяжелый багаж. Он замедлит ваше движение и затормозит поток эвакуируемых. Ни в коем случае не возвращайтесь в здание за своими вещами. Если вы плохо знаете здание или не говорите на местном языке, следуйте за толпой и не идите навстречу общему потоку. Держитесь правой стороны в коридорах и на лестницах, чтобы не мешать проходу пожарных и работников аварийных служб.

• Продукты горения очень токсичны, и от них гибнет много людей. Если источник пламени находится на нижних этажах, то дым поднимается вверх и заполняет верхние этажи. Иногда ничего не остается, как ждать помощи, но иногда срочная эвакуация имеет первостепенное значение, если на нижних этажах сильный пожар.

• Если помещение наполнилось дымом, прижмитесь к полу и ползите к ближайшему аварийному выходу. В случае сильного пожара может автоматически включиться система огнетушения. Тогда видимость может даже ухудшиться, и гладкие поверхности станут еще более скользкими.

• При чрезвычайной ситуации подумайте, стоит ли остановиться, чтобы помочь другим. Помните, что продукты горения очень быстро действуют даже на крепкий организм. Можно поместить пострадавших в какое-нибудь безопасное место, а затем сообщить соответствующим службам спасения об их местонахождении.

• Покинув здание, идите к месту аварийного сбора. Если вы считаете, что там опасно, покиньте эту территорию.

• Оказавшись в безопасности, свяжитесь со своим офисом и семьей.

В случае угрозы взрыва в городе:

• К каждой угрозе относитесь серьезно, даже если до этого были ложные сообщения о заложенных взрывных устройствах. Если вы едете с группой, каждый должен знать, как себя вести.

• Если вас предупредили о наличии взрывного устройства, постарайтесь понять, где оно находится и когда предположительно взорвется. Тогда можно оценить, сколько в вашем распоряжении времени на эвакуацию.

• Если по вашим расчетам времени на эвакуацию достаточно, выходите по указателям аварийных выходов. Не пользуйтесь лифтом. В любой момент он может быть отключен, и вы застрянете между этажами. В такой ситуации может понадобиться время, чтобы вызволить вас оттуда.

• Во время эвакуации имейте в виду, что по соседству могут быть заложены другие взрывные устройства. Избегайте подозрительных свертков, мусорных урн, припаркованных в неположенном месте автомобилей и т. п. Положитесь на свою интуицию. Если что-то выглядит подозрительным, держитесь от этого подальше.

• Если на эвакуацию нет времени, перейдите в часть здания, удаленную от взрывного устройства, и попытайтесь найти помещение без окон. При взрыве осколки стекол действуют, как осколки снарядов, и могут нанести серьезные ранения. Кроме того, стекло не видно при просвечивании рентгеновскими лучами и может остаться незамеченным при медицинском осмотре.

• Старайтесь, чтобы между вами и взрывным устройством было как можно больше препятствий, таких, как стены и большие письменные столы. Спрячьтесь под стол и оставайтесь там, пока не произойдет взрыв. Накройте голову руками, книгами, пачками бумаги и другими материалами, оказавшимися под рукой. Закройте рот, но приоткройте челюсти, чтобы не повредились барабанные перепонки при сильном взрыве.

• Тактика террористов — заложить одновременно несколько взрывных устройств, чтобы вызвать максимум жертв. Взрыв одного из них вызовет панику среди людей, покидающих здание. Второй взрыв поразит эвакуируемых. Поэтому лучше оставаться там, где вас застал первый взрыв, если только не начнется сильное задымление или пожар.

• Многие взрывные устройства подрываются посредством дистанционного управления. Террористы подают радиосигнал, вызывающий детонацию. Поэтому при угрозе взрыва не пользуйтесь радиотелефоном или портативным радиоприемником, так как они могут неумышленно вызвать преждевременную детонацию взрывного устройства.

• В некоторых странах наблюдается значительный рост терактов с участием террористов-смертников. Не исключено, что подобная практика будет использоваться в деловых центрах. При поездках в неспокойные регионы или при посещении международных деловых центров в периоды напряженности будьте внимательны на больших публичных собраниях. Политические и даже общественные мероприятия в некоторых странах оказались под прицелом террористов-смертников. Изучите в буклете отеля, какие намечаются мероприятия, и поинтересуйтесь, каковы меры безопасности.

• Главная цель террористов всего мира — посеять хаос. Поэтому в крупных деловых центрах теракты совершаются в часы пик. Переполненные вокзалы или станции метро, стоянки такси или автобусные остановки — все они подвергались терактам. В неспокойных регионах или в период обострения ситуации не пользуйтесь общественным транспортом в часы пик.

Коммерческий шпионаж существует не только на страницах детективных романов. Деловые люди в зарубежных поездках несут важную коммерческую информацию, и зарубежные конкуренты и даже государства готовы на экстремальные меры, чтобы ее заполучить. За деловыми людьми во время их зарубежных командировок устанавливают слежку их конкуренты, службы безопасности, банды террористов, криминальные элементы и даже сред-

ства массовой информации, заинтересованные в установлении контактов с правительственными органами и бизнесом.

Во время заграничной командировки постоянно помните, что за вами могут следить и что ваша повседневная жизнь, контакты и деятельность находятся под наблюдением.

Слежка — это не только следование за вами повсюду сомнительных личностей. Современные высокие технологии позволяют легко прослушивать ваши телефонные разговоры и частные беседы, перехватывать послания, переданные по электронной почте и по факсу. Поэтому оцените свои наиболее уязвимые места, затем измените тактику своего поведения и примите меры безопасности.

Особо важно понять, какая информация представляет наибольший интерес для ваших преследователей, и особенно тщательно ее защищайте. И конечно, надо уметь выявлять **признаки повышенного интереса к вашей деятельности.**

• Вас должно насторожить, если кто-то, не связанный с вашим бизнесом или не имеющий отношения к вашей фирме, часто подходит к вам, проявляя повышенный интерес к вашей деятельности в их стране. Обычная уловка — спросить, знаете ли вы некую персону, работающую в вашем бизнесе. Будьте осторожны, если незнакомец интересуется вашим гражданством. Опасайтесь тех, кто представляется изучающим английский язык и желающим попрактиковаться.

• Дважды подумайте, прежде чем принять деловое предложение от незнакомцев, не связанных с вашей компанией. На вечеринках, обедах и других мероприятиях избегайте разговоров о вашей деятельности. Ограничьте употребление алкогольных напитков. В щекотливых ситуациях сами заказывайте себе выпивку, чтобы не обидеть отказом предлагающих вам выпивку незнакомцев. Всегда имейте полный бокал.

• Будьте осторожны в контактах с официальными лицами иностранного государства, правоохранительными органами или военными организациями. Это особенно важно при внутреннем конфликте в стране или напряженности на границе.

• Остерегайтесь местных женщин, которые пытаются вступить с вами в беседу или просят купить выпивку в баре отеля.

• Обнаружив вокруг себя подозрительную активность людей или автомобилей, наводящую на мысль о слежке, сделайте вид, будто ничего не замечаете, и продолжайте обычную жизнь, но будьте осторожны в своих действиях и высказываниях. Если вы не выдержите и попытаетесь сбежать, они могут подумать, что вам есть что скрывать, и активизируют свои усилия. В экстремальных случаях, или если у вас какой-то особый бизнес, стоит прервать командировку и вернуться домой.

• Успешное наблюдение — нелегкая задача. Необходимы квалифицированные сыщики и люди среднего звена, чтобы координировать преследование быстро перемещающейся цели. Если ваша работа такова, что вы ощущаете, что за вами может вестись профессиональное наблюдение, обратите пристальное внимание на циркулирующие поблизости автомобили, на водителей, проявляющих повышенный интерес к вам, вашей машине и отелю. Плохо обученные группы, осуществляющие наблюдение, легко выделяются из толпы, так как применяют грубые методы. Они могут разглядывать витрины магазинов на противоположной стороне улицы, наблюдая за вашим отражением, ехать за вами в машине с затененными стеклами или просто выглядеть подозрительно.

• Опытный сыщик может быть мужчиной, женщиной или ребенком. Доверяйте своей интуиции. Записывайте тайком номера машин или приметы следящих за вами людей и сообщите об этом в посольство или консульство и в свою фирму.

• Если вы будете совершать одни и те же действия каждый день в одно и то же время, за вами будет легко вести слежку. Будьте немного непредсказуемым. Держите в тайне свое расписание и договаривайтесь о встречах только по надежным каналам.

• Будьте осторожны, назначая деловые свидания на семинарах, выставках или импровизированных встречах. Такая встреча могла быть специально организована, чтобы подслушать вашу беседу.

• Если вам нужно поговорить по телефону, отправить послание по электронной почте или по факсу из отеля, помните, что их могут перехватить. Не отправляйте важных материалов. В отелях многих стран используются устаревшие средства связи.

• Если у вас возникли подозрения, что в вашем номере имеются прослушивающие электронные устройства, поменяйте номер. Если вы найдете такое устройство и уничтожите его, то только усилите подозрение. Не ведите деловых разговоров из своего номера.

• Не оставляйте важных посланий на автоответчике или голосовой почте мобильного телефона. Эти устройства легко доступны группе наблюдения. Диктофон — надежное средство хранения информации в поездке, если, конечно, он не попадет в чужие руки.

• В факсимильных аппаратах для печати используется бобина черной пленки, которая, по сути, является копией всех полученных вами посланий. Не выбрасывайте ее. Ожидая важное послание из вашего офиса, договоритесь, чтобы оно пришло тогда, когда вы будете на месте (с учетом разницы во времени). Иначе информация может попасть в чужие руки.

• Портативные компьютеры стали важной принадлежностью деловых людей, но они могут сделать их уязвимыми для сыщиков. Были сообщения о преступных группах с видеокамерами, на которые тайком снимались электронные послания, когда бизнесмены набирали их на своих ноутбуках. Такую видеозапись можно расшифровать и узнать содержание послания. Люди, сидящие с вами рядом, могут подглядеть печатаемый вами текст. Убедитесь, что за вами никто не подглядывает, прежде чем набирать важный материал на ноутбуке.

• Отправляясь в поездку, проверьте, чтобы на жестком диске была только абсолютно необходимая информация. Сделайте копии самых важных файлов и удалите всю персональную информацию. Некоторые вынимают жесткий диск и кладут его в карман, а затем устанавливают обратно. По прибытии в аэропорт элементы пита-

ния вашего ноутбука должны быть заряжены. Были случаи, когда ноутбуки, которые не удалось включить, были конфискованы по подозрению, что они содержат взрывное устройство.

• При отъезде ничего не оставляйте, а поместите в запирающийся кейс. Не бросайте все подряд в мусорную корзину. Из того, что вы выбросите, можно будет извлечь информацию. Группа, осуществляющая наблюдение за вами, всегда исследует содержимое мусорных корзин в поисках важных материалов, таких, как заметки о вашей командировке. Лист чистой на вид бумаги может нести на себе отпечаток того, что вы писали на верхнем листе. На чеках может быть номер вашей кредитной карты. На использованных авиабилетах указано название авиакомпании, что позволит изучить расписание полетов и догадаться, когда вы собираетесь улететь. Потенциальные похитители могут проследить ваш маршрут.

4.2. Личная безопасность

Поездка сама по себе может быть напряженной, и многие безобидные виды деятельности могут привести к потенциально взрывной ситуации. Например, вы стоите в длинной очереди за билетами. Подходит местный житель и покупает билет без очереди. Это может вывести из себя, но это один из многих местных обычаев, которые иностранец должен научиться принимать. Многие из этих ситуаций можно мирно разрешить при надлежащем подходе.

Умение выйти из напряженной ситуации поможет быстро принять решение и предотвратить опасные инциденты. Выработайте стратегию выхода из кризисной ситуации. При поездке в потенциально опасный регион эта стратегия должна включать три элемента: осознание опасности, создание дистанции вокруг себя и бегство.

Осознание скрытой опасности в вашем окружении во время поездки или пребывания в чужом городе очень важно. Нужно понять стандарты поведения местных жителей, чтобы осознать потенциально опасную ситуацию, а для этого надо знать мест-

ные обычаи и образ жизни. Прислушивайтесь также к вашей интуиции.

Если вас встревожила ситуация или отдельный человек, внутренний голос подскажет вам, что надо ретироваться. И если вы оказались втянутым в ситуацию, когда возможно нападение, осознание степени риска поможет принять быстрое решение. Не стоит рисковать жизнью из-за чего-то, что легко возместить, и лучшим выходом, например, будет отдать бумажник или камеру.

Если вы оказались в состоянии конфронтации, создайте вокруг себя безопасное пространство. Попытайтесь удерживать нападающего на расстоянии вытянутой руки. Если он попытается нарушить эту дистанцию, отодвиньтесь, чтобы ее сохранить. Можно поднять голос, чтобы его отпугнуть или привлечь внимание окружающих.

Примите уверенную позу, смотрите ему в глаза и громко и твердо скажите, что понимаете, чего он хочет, и что это не пройдет. Преступники обычно выбирают слабых, и, если вы окажете сопротивление, они отступят и будут искать другую жертву.

Если они не отступят и будут приближаться к вам, возможно, придется отдать то, что они требуют, или попытаться убежать. Крайнее средство — попытка применить силу, и вы должны показать нападающему, что вы это сделаете.

Последний элемент стратегии — бегство. Он тесно связан с первым элементом — осознанием опасности. Нужно знать, где находятся безопасные места — освещенные кафе, полицейские участки, больницы. Если вы примете решение к бегству, то должны знать, куда бежать.

4.2.1. Контроль ситуации

Многие нападения можно предотвратить, если жертва почувствует признаки опасности или будет знать, как развиваются подобные ситуации. Люди, предрасположенные к насилию, не нападут на тех, кто контролирует ситуацию. Они ищут признаки слабости и неуверенности. Исходя из здравого смысла, приняв простые

меры предосторожности и ведя себя уверенно, можно снизить риск стать жертвой.

• В поездке по опасному региону наймите местного гида через своего турагента или администрацию отеля. Гид знаком с ситуацией и знает, как уладить проблемы. Однако следует осознавать, что этот человек связан со своими соотечественниками, соседями, друзьями, семьей. Он не будет целиком на вашей стороне, поэтому соблюдайте дистанцию: никогда не посвящайте его целиком в свои планы, только в пределах вежливости, и не рассказывайте ничего о себе.

• Старайтесь выглядеть спокойным и уверенным в себе, покажите, что можете постоять за себя. Всегда будьте начеку, контролируйте, что происходит вокруг, и выработайте стратегию, как держать себя. Уйдите с места назревающего конфликта или останьтесь среди людей, чтобы снизить риск.

• Если вы оказались в конфликтной ситуации, дайте понять, что вы слушаете, что вам говорят, не прерывайте на середине фразы. Даже если вы — пострадавшая сторона, сопротивляйтесь желанию силой отстаивать свою точку зрения. Постарайтесь лучше вникнуть в суть конфликта — это позволит понять позицию другого человека и будет способствовать разрешению конфликта.

• Если вы попали в ДТП, в котором вы можете быть полным или частичным виновником, признайте свою вину и не обвиняйте других. Однако при некоторых обстоятельствах, даже если вы виноваты, не принимайте на себя ответственность, пока не обратитесь за советом к адвокату. Пойдите на компромисс с другими сторонами конфликта, чтобы не унизить их.

• Подумайте о последствиях ваших действий. Ваша собственная реакция на напряженную ситуацию может сказаться на реакции других. Если вы пойдете на конфронтацию, то получите такую же ответную реакцию. Лучше удалиться или пойти на компромисс.

• Старайтесь не унижать других. Это очень важно в некоторых регионах мира. В обществе, где главенствуют мужчины, для них — удар по их чести, если они будут выглядеть глупо, и это неизбежно

приведет к насилию. Даже если человек не прав, проявите уважение к нему и его позиции.

• Не комментируйте национальную, этническую или религиозную принадлежность. Не отвечайте на выпады. Старайтесь не обострять ситуацию.

• При некоторых обстоятельствах юмор позволит разрядить обстановку. Например, если вы прикинетесь униженным и будете изображать глуповатого туриста, это может смягчить гнев обиженного вами человека. Однако помните, что есть вещи, над которыми нельзя шутить. Это религия, культурные традиции, местные обычаи, политическая система, национальные лидеры. В некоторых странах местным жителям, но не иностранцам, позволено подшучивать над некоторыми вещами. Овладейте этим искусством.

• Не ведите себя надменно и невежливо.

• На улице вас останавливают вовсе не те, с кем вам хотелось бы пообщаться. Во многих странах таких людей интересует лишь одно — деньги. Не вступайте с ними в разговор. Иногда бывает достаточно просто сказать им "нет". Сконцентрируйте внимание на своем маршруте и не заговаривайте ни с кем, если подозреваете какую-то опасность.

• В условиях международной напряженности не в ваших интересах афишировать свою национальность. Если вас втянут в дискуссию о внешней политике вашей страны, старайтесь улыбаться и согласитесь, что ваша страна проводит неправильную политику. Даже если вы с этим не согласны, это может разрядить обстановку.

4.2.2. Преступность

Преступность существует везде. Это глобальная проблема, и куда бы вы ни приехали, будьте готовы к встрече с криминальной активностью. Некоторые страны не предоставляют полных данных о преступлениях против туристов, чтобы защитить свой туристический бизнес. Однако в большинстве стран уровень преступности значительно вырос.

Чтобы не стать жертвой преступления, обратите внимание на следующие правила безопасности:

• За границей придерживайтесь тех же правил безопасности, что и дома. Помните, что излюбленные места преступников — переполненные терминалы общественного транспорта, уличные шествия, достопримечательности, посещаемые туристами, базары под открытым небом, "улицы красных фонарей".

• В некоторых странах избегайте мест отправления религиозных культов. Религия связана с сильными эмоциями, и религиозные фанатики могут прийти в состояние сильного возбуждения даже при малейшем намеке против их религии. Узнайте, где находятся места религиозных поклонений, и держитесь от них подальше в дни религиозных праздников.

• Изучите окрестности. Узнайте, какие магазины, бары и рестораны открыты большую часть суток. Если вам известен повседневный режим жизни и он по какой-то причине изменился, то вы это заметите.

• Возьмите мобильный телефон, подключенный в месте вашего назначения, и всегда носите его с собой. Если нет такой возможности, узнайте, где находится ближайший телефон-автомат, научитесь им пользоваться. Купите карточку местной телефонной сети или запаситесь достаточным количеством монет для звонка в службы скорой помощи.

• Когда вы идете по улице пешком, проверьте, не преследует ли вас медленно движущаяся машина или какие-то неизвестные люди. Избегайте незнакомых мест и глухих дорог. Туристические зоны выглядят ухоженными и благополучными. Но если вокруг мрачная, плохо освещенная территория, неприглядные дома с разрисованными стенами, возможно, вы попали в неблагополучный квартал. Не углубляйтесь туда, а поскорее покиньте это место.

• Во время длительной командировки установите добрые отношения с соседями. Подружившись с живущими рядом, вы установите своего рода сеть тревожной сигнализации. Местные жители лучше подготовлены к возможным опасностям, чем вы. Они, к примеру, могут определить подозрительных людей и

машины. Но они могут сообщить вам и об изменениях ситуации, если с вами знакомы.

• Держите людей в курсе ваших перемещений, сообщите друзьям и коллегам, куда собираетесь, когда там будете и когда вернетесь. Сообщите им свой маршрут и вид транспорта. Если вы не вернетесь, они будут знать, что надо действовать.

• Расскажите о своих приготовлениях к поездке только тому, кому это положено знать. Не давайте никому номер телефона, домашний адрес и финансовую информацию, например какой кредитной карточкой вы пользуетесь. Многие по возвращении домой получают счета на оплату, потому что их финансовые реквизиты попали в чужие руки.

• В местах с высоким уровнем насилия узнайте самые опасные места. Не подвергайте себя риску на темных, плохо освещенных улицах. Не старайтесь сократить дорогу до торгового центра и обратно. Преступники часто прячутся в таких местах, чтобы ограбить приезжих с толстыми бумажниками. Избегайте длинных узких улиц.

• Не задерживайтесь около банков и обменных пунктов в чужом городе, не подходите ночью к банкоматам. Преступнику нетрудно заметить, что вы воспользовались своей кредитной карточкой и имеете наличные деньги.

• Мелкие преступники, такие как карманные воришки, часто работают в организованных группах, которые могут контролировать обширную территорию. Они орудуют главным образом в городе и встречаются в условленных местах, чтобы поделить добычу. В чужом городе помните, что этот вид преступления вездесущ, и будьте бдительны. Известная уловка карманников — вас втягивают в разговор, спрашивая дорогу или время, а их сообщник как бы случайно налетает на вас, быстро выхватывает бумажник или сумочку во время возникшей сумятицы. Остерегайтесь отвлекающих внимание уличных сцен, таких как драка или громкая ссора. При виде таких сцен держите свои ценные вещи.

• Будьте осторожны с предложениями, которые кажутся слишком заманчивыми, чтобы быть правдой. Если кто-то на

улице предлагает вам услуги по ценам гораздо ниже принятых, будьте начеку. Либо вам придется заплатить за посреднические услуги, либо вы станете жертвой мошенников.

• Преступники часто выжидают подходящий момент. Один из таких моментов — когда вы приближаетесь к своему автомобилю или дому. Проверьте, что никто не околачивается поблизости. Если вы испытываете чувство страха, вернитесь. Подходя к дому или к машине, держите ключи наготове. Если вы остановитесь, чтобы достать ключи, то предоставите преступникам возможность, которой они воспользуются.

• Возвращаясь домой с покупками, не нагружайте себя свертками и пакетами. Это тот самый момент, которого ждут преступники. Безопаснее нанять такси, которое довезет вас до самых дверей.

• Многие отели предлагают сопровождающего, когда вы идете за покупками. Он обеспечит вам приемлемые цены, а также будет оберегать от всяких неприятностей.

• Если вы стали жертвой преступления и у вас украли паспорт, дорожные чеки и ценные вещи, незамедлительно обратитесь в полицейский участок. Вам может понадобиться справка для обращения в страховую компанию. В некоторых странах это не так просто, у туристов требуют плату за каждую бумажку. Обговорите процедуру со страховой компанией.

• К туристам придираются без всякой видимой причины или за неумышленное нарушение местных законов. В такой ситуации имеет смысл извиниться и попытаться оправдаться. Однако если нападки не прекратятся, дайте отпор. Скажите громко и уверенно, чтобы вас оставили в покое, иначе вы вызовете полицию.

• Оказание сопротивления грабителям — законное действие. Если вы стали жертвой преступника, значит, он рассчитывал на успех. В таких случаях вас, вероятно, вычислили, или преступник в отчаянии решился на такой поступок. Если вы часто попадали в такие ситуации, возможно, вам захочется оказать сопротивление. Но многие считают, что ради вещей не стоит рисковать жизнью.

• Некоторые приобретают оружие, чтобы защитить себя. Но тогда они могут еще сильнее рисковать, полагая, что готовы к неприятностям. Что произойдет, если вы решите им воспользоваться? Ситуация может стать взрывной и даже более опасной. Каковы законы, касающиеся использования оружия, в данной стране? Это может привести к серьезным неприятностям. Безопаснее оставаться невооруженным.

4.2.3. Коррупция

Во многих странах взятка — это образ жизни, и ожидается, что иностранные туристы будут платить. Полицейские, военные, таможенники, иммиграционные службы, общественный транспорт, правительственные чиновники пополняют свои доходы за счет западных туристов, и, отказавшись платить, вы попадете в бесконечный бюрократический кошмар. Отказ или неспособность заплатить могут привести к аресту под надуманным предлогом и испортить деловую поездку или отпуск. Коррупция широко распространена и не ограничивается социально неблагополучными регионами.

Но давать взятки приходится и местным жителям. Мелкие взятки — общее правило для многих регионов мира, и местные чиновники ежедневно обманывают местных жителей. Когда это пустило глубокие корни, о морали не может идти и речи. Если вы попытаетесь сказать таможеннику с мизерной зарплатой, что его поступок противозаконен, весьма вероятно, что вы пожалеете о том, что отказались заплатить 20 долларов, после того, как вас продержат несколько часов в маленькой камере.

Небольшие дорожные происшествия — другой способ получения денег с туристов. Разбитое боковое зеркало или выключенные огни даже на дорогах, где машины едут без огней, могут привести к штрафу.

Однако важно знать, что не все чиновники коррумпированы. Если вы попытаетесь дать взятку честному чиновнику, то можете получить длительный срок в местной тюрьме. Нужно научиться читать подаваемые вам знаки.

Следующие рекомендации позволят вам разобраться, нужно ли давать взятку в данной ситуации и как общаться с коррумпированными чиновниками.

• Не предлагайте чиновнику взятку автоматически, как только вас остановили. Пусть он подаст вам знак. Если он старается решить дело и вступает с вами в разговор, не пытаясь задержать, значит, он ожидает наличных.

• Принято платить "штраф" на месте. Однако можно сэкономить наличные, если знать таксу. Иногда вам вручат бесполезный кусок бумаги под видом квитанции. Знайте, что в такой ситуации шутки неуместны.

• Обычный прием — найти проблему, например, с вашими документами, которая требует длительного решения. Чиновник скажет, что знает выход из положения, но для этого требуются время и деньги. Здесь ваша очередь спросить, сколько потребуется времени и сколько это стоит. Затем можно доверительно спросить новообретенного "друга", не мог бы он лично заняться вашим делом. Заплатите, сколько он попросит, если не слишком много.

• Не существует тарифа взяток коррумпированным чиновникам — это устанавливается методом проб и ошибок. Они хотят получить как можно больше, а вы — заплатить как можно меньше. Лучше всего поинтересоваться у тех, кто здесь живет. Помните, что в некоторых регионах взятка — это образ жизни, и ее надо включать в бюджет поездки.

• В случае серьезных инцидентов требуются большие деньги. Чем выше должностные лица, тем выше тариф. Если вам грозит тюрьма, придется заплатить серьезную сумму.

• Прибытие в страну с компьютером и какими-то необычными устройствами также может послужить поводом для взятки. Устройство, неизвестное таможенным чиновникам, может быть подвергнуто неожиданному тщательному изучению. Они могут заявить, что это устройство запрещено к ввозу в страну, даже если не знают, что это такое. Будьте осторожны. Некоторые добросовестно делают свою работу, но коррумпированные чиновники быстро дадут вам о себе знать.

• Экспатрианты, достаточно долго живущие в стране, иногда имеют связи среди верхушки местных властей и опыт общения с полицейскими и военными. Но туристы более уязвимы, и их легче запугать, особенно в аэропорту перед вылетом. Попробуйте сделать вид, что вы живете в этой стране. Если вы торопитесь, упоминания имени какого-нибудь местного политического деятеля или влиятельного бизнесмена может оказаться достаточно, чтобы отпугнуть взяточника.

• Иногда у вас могут потребовать слишком высокую взятку, особенно молодые полицейские и солдаты, пытающие удачу. На этот случай необходимо иметь небольшую сумму наличных. Покажите, что у вас в бумажнике мало денег. Однако они могут забрать все, поэтому не держите в бумажнике кредитные карты.

• Направляясь в некоторые страны, особенно находящиеся в состоянии гражданских волнений и войны, можно взять какие-то вещи, которые помогут преодолеть преграды. В зависимости от страны можно, например, взять блок сигарет. Такса в военной зоне — пачка сигарет "Мальборо". В некоторых странах бутылки спиртного может быть достаточно, но держитесь подальше, пока они будут пить. Консервы, туалетные принадлежности, дешевые солнцезащитные очки и другие мелкие подарки помогут договориться с коррумпированными полицейскими и военными на контрольно-пропускных пунктах.

4.2.4. Наркотики

В оборот наркотиков вовлечены миллионы людей, употребляющих их и распространяющих во всем мире. Это большой бизнес, и ставки чрезвычайно высоки, поэтому неудивительно, что многие люди хотели бы вас туда вовлечь.

Когда кто-то предлагает вам способ быстрого обогащения, знайте, что это всегда ловушка. Если вам предлагают продавать и переправлять наркотики, то несколько лучших лет жизни вы можете провести в тюрьме.

Во многих странах вам предложат гашиш и марихуану, используемые там регулярно, хотя теперь осталось мало стран,

где они узаконены. Даже несмотря на то, что "все употребляют", у местной полиции к иностранцам может быть особое отношение, по крайней мере, как к источнику дохода.

Во многих странах наказание за хранение наркотиков почти такое же, как и за распространение. Во всяком случае, если вас поймают, вам придется иметь дело с местной полицией в ситуации не из приятных, и в лучшем случае придется дать крупную взятку, чтобы вас отпустили.

• Имейте в виду, что в ваш номер отеля могут быть подброшены наркотики, особенно если вы останавливаетесь в общежитии или дешевом отеле. Проверьте ваш номер, посмотрите под матрасом, за ящиками стола, в бачке и других укромных местах. Если что-нибудь найдете, незамедлительно избавьтесь, спустив, например, в туалет, и смените отель. Если вас поймают в номере с наркотиками, даже если вы не знали об их существовании, то вы можете попасть в тюрьму.

• Переполненные терминалы аэропорта — также зона риска для ничего не подозревающих пассажиров. Одна из уловок — оттереть вас от вашего багажа и сунуть туда маленький пакетик. Их намерение — следить за вами, пока вы не пройдете таможенный досмотр, и забрать ваш багаж в месте назначения. Не спускайте глаз со своего багажа.

• Если вам по состоянию здоровья необходим какой-то медицинский препарат, храните его в оригинальной упаковке и постарайтесь получить у вашего лечащего врача сертификат, позволяющий иметь при себе это лекарство. Некоторые чиновники относятся очень подозрительно даже к прописанным лекарствам и могут вас задержать.

• Если у вас диабет или другая болезнь, требующая инъекций, получите у лечащего врача сертификат, позволяющий иметь при себе шприцы. По очевидным причинам шприцы привлекают к себе повышенное внимание.

4.2.5. Фотографирование

Наличие фото- и видеоаппаратуры может создать проблемы за рубежом. В некоторых странах, особенно неспокойных, могут

быть другие меры безопасности. Если вас поймают за фото- или видеосъемкой некоторых объектов, вас могут задержать и конфисковать аппаратуру и пленку или даже посадить в тюрьму.

В некоторых странах существуют очень строгие запреты на фотографирование. Запрещается фотографировать и снимать на видео приграничные области, уличные манифестации или беспорядки, полицейских и военных и их технику, гавани, железные дороги и аэропорты.

Запрет может распространяться на мосты, общественные и правительственные здания (например, резиденцию президента), аэропорты, плотины, электростанции и все, что может рассматриваться как цель для нападения. В некоторых странах запрещено фотографировать бедных и трущобы.

Если существуют строгие правила, они обычно вывешиваются на пограничных переходах и в аэропортах и иногда непосредственно на объектах, запрещенных для фотографирования. Общее правило — не фотографируйте никаких официальных объектов, особенно военных. Если место охраняется, спросите охранников, можно ли фотографировать.

В некоторых местах правила иногда вольно толкуются не в меру усердными солдатами, чтобы придраться к туристам.

Если вас задержали, будьте вежливы, извинитесь, сказав, что не видели никакой опасности в фотографировании красивого здания железнодорожного вокзала. Если это не подействует, спокойно отдайте пленку, иначе могут разбить камеру.

В регионах с религиозными конфликтами не фотографируйте места религиозных поклонений.

4.2.6. Правовая система

Покидая свою страну, вы попадаете в правовое поле чужой страны. Поэтому постарайтесь больше узнать о местных законах. Сходите в библиотеку, расспросите турагента, работников посольств и консульств или сотрудников туристических бюро страны, куда вы собираетесь в поездку. Следите за публикациями в прессе.

В другой стране вас могут арестовать за действия, которые абсолютно законны или считаются мелким нарушением в вашей стране. Узнайте, что считается преступлением в стране, куда вы едете. Это особенно важно при поездках в страны ислама, где религия определяет закон. Например, в Саудовской Аравии употребление алкоголя карается высоким штрафом.

Люди, покупающие антикварные предметы в некоторых странах, таких как Турция, Египет, Мексика, рискуют быть арестованными. Местные таможенники могут отнести эти предметы к национальному достоянию. В таких странах на каждую копию, купленную в магазине, нужно иметь документ. Если предмет подлинный, необходимо получить разрешение на вывоз (обычно в национальном музее).

При въезде в страну с другой идеологией убедитесь, что литература, которую вы везете с собой, не может считаться подстрекательской.

Во многих странах имеются ограничения на сумму вывозимых из страны наличных денег. Узнайте валютные правила в стране, куда вы едете.

В настоящее время туристы подвергаются тщательному досмотру на предмет ввоза запрещенной мясной или молочной продукции. При обнаружении незаконных продуктов налагается высокий штраф. Наведите справки в местном консульском отделе страны, в которую вы едете.

4.3. Авиаперелет

4.3.1. Безопасность в аэропорту

Запомните следующее, чтобы избежать инцидентов в аэропорту.

• Приезжайте в аэропорт заранее, чтобы было достаточно времени для прохождения контроля. В большинстве авиакомпаний регистрация начинается за два часа до отлета. Однако при большом наплыве пассажиров возможны задержки. Если вы путешествуете с группой, то приезжайте еще раньше. Для прохождения

контроля семьей или группой студентов требуется больше времени, чем для индивидуального туриста.

• Контроль может проходить очень медленно. Это необходимые меры предосторожности, но вы почувствуете нарастающее напряжение, если рейс будет задержан. В такие моменты аэропорты могут стать генераторами стресса, полными раздраженных пассажиров. Избегайте всяких препирательств, особенно в жаркую погоду. Держитесь подальше от людей в состоянии алкогольного опьянения. Сочетание избытка алкоголя и задержки рейса особенно опасно.

• Выбирайте ранний утренний рейс. Чем раньше вы улетите, тем меньше вероятность задержки.

• Перед выездом в аэропорт проверьте, что взяли все необходимые документы. При полете с группой лучше иметь руководителя, у которого будут находиться все документы. После прохождения контроля идите прямо к своему выходу.

• Безопасное место находится в зоне между входом для прибывших и выходом для улетающих. Когда в накопителе много народу, лучше не ходить в магазины и кафе вне этой площади.

• В аэропорту не спускайте глаз со своего багажа. Нередко в багаж ничего не подозревающих пассажиров подкладывают запрещенные для провоза вещи, например наркотики.

• Никогда не берите чужой багаж, даже лучшего друга. Если нет выхода, обязательно скажите при прохождении контроля, что несете чужой багаж.

• Если увидите бесхозный багаж или свертки, держитесь от них подальше — там может быть взрывчатка. Точно так же, если вы оставите свой багаж без присмотра, его могут забрать, открыть и даже уничтожить направленным взрывом. Держитесь подальше от урн для мусора — в них могут подложить взрывные устройства. В ряде стран на железнодорожных вокзалах и в аэропортах по этой причине нет урн.

• Никогда не говорите в шутку, что у вас в багаже бомба или огнестрельное оружие. Вас воспримут всерьез и арестуют, и это скажется на других пассажирах, так как весь багаж будет выгружен, чтобы найти ваш.

• При поездках с детьми не отпускайте их от себя. Некоторые международные аэропорты притягивают преступников.

• Не думайте, что каждый в форме носильщика действительно работает в аэропорту. Здесь легко ошибиться. Такой лженосильщик может исчезнуть с вашим багажом. Особенно внимательны будьте вне аэропорта. Здесь может быть много мошенников, желающих поживиться за счет туристов.

• Из-за угрозы взрывов службы безопасности некоторых аэропортов могут уничтожить подозрительные автомобили направленным взрывом. Убедитесь, что ваш автомобиль припаркован легально, иначе в лучшем случае он будет эвакуирован.

• По возвращении из поездки у вас должна быть достаточная сумма денег, чтобы расплатиться. В противном случае ваш автомобиль может быть конфискован.

• С аэропортовских стоянок автомобили часто угоняют. Проверьте, чтобы все замки были заперты, а окна плотно закрыты. Около 50% всех угнанных автомобилей были плохо закрыты. Не забудьте взять ключ. В 20% угнанных автомобилей были оставлены ключи. Никогда не оставляйте запасные ключи в автомобиле или около него. Запасные ключи преступнику легко найти. Если есть место около охранника, припаркуйтесь там. Это отпугнет потенциального угонщика.

• Избегайте рейсов с промежуточной посадкой в неспокойных регионах. Такие рейсы могут быть дешевле, но более доступны террористам и криминальным элементам.

• Слушайте объявления службы безопасности аэропорта. Если необходима эвакуация, сообщение будет передано по внутренней радиосети. Следует сориентироваться, в каком месте аэропорта вы находитесь и где выход.

• Уважительно относитесь к работникам таможенной и пограничной служб. Иногда трудно сдержаться, но помните, что в современной обстановке не далеко до беды. Известны многочисленные примеры, когда служащие аэропорта обращались с пассажирами не лучшим образом. В любом случае будьте вежливы и терпеливы.

• В некоторых регионах принято давать взятки таможенникам и иммиграционным служащим. В такой ситуации спросите себя, стоит ли наживать неприятности. Разумеется, вы не должны платить, но последствия могут быть еще хуже.

• Когда ваш багаж находится на конвейерной ленте рентгеновского контроля, не спускайте с него глаз. Сейчас жулики часто используют такую уловку. Шайка жуликов располагается впереди и сзади вас. Когда ваш багаж появляется с другой стороны, жулик берет его и одновременно подкладывает металлический предмет. Пока служба безопасности проводит проверку, жулик беспрепятственно скрывается с вашим багажом.

4.3.2. Выбор места

Многие пытаются определить, какие места наиболее безопасны на борту самолета. Но характер авиакатастрофы непредсказуем, и трудно угадать, какие места дают шанс выжить. Нет оснований считать, что какая-то часть самолета безопаснее во время полета, чем другие. До сих пор самую большую опасность представлял упавший с багажной полки багаж.

Бронируя места, примите во внимание следующие факторы:

• Не исключено, что полет на широкофюзеляжном самолете снижает риск террористического инцидента. "Боинг-747" и другие большие самолеты могут приземляться только на специальных аэродромах, и это снижает опасность теракта. Большое число пассажиров на борту широкофюзеляжного самолета — также препятствие для банды террористов, так как требуется много людей, чтобы контролировать ситуацию. Частично заполненный "Боинг-747" менее привлекателен для некоторых террористов, поэтому постарайтесь оценить ситуацию.

• Не выбирайте место рядом с проходом. Многие предпочитают эти места в надежде, что можно будет встать и пройтись по салону при длительном полете. Однако здесь вы лучшая мишень при любом инциденте. При теракте и любом воздушном происшествии больше всего страдают пассажиры, находящиеся вблизи прохода.

• Если вы путешествуете вдвоем, забронируйте одно место у окна, а другое — у прохода. Тогда место между вами может оказаться свободным. Эти места бронируются в последнюю очередь, и если самолет не будет заполнен, то вам будет просторнее.

• При бронировании билета попросите у кассира схему мест. Можно посмотреть план салона в Интернете на сайте авиакомпании и узнать, какие места находятся рядом с аварийным выходом. Здесь больше места между рядами, так что можно вытянуть ноги.

• Если ваши места рядом с аварийным выходом, внимательно изучите инструкцию, как открыть дверь. Если вы не можете понять механизм ее действия, то подвергаете опасности не только себя, но и остальных пассажиров. Эта дверь тяжелая, и нужно быть физически сильным, чтобы ее открыть. Оцените свои возможности. Если вы не сможете справиться с дверью, то лучше поменяться местами с тем, кому это по плечу.

• Независимо от того, где ваше место, узнайте, где находится ближайший аварийный выход. Запомните направление и посчитайте, сколько до него рядов, чтобы смочь пройти туда даже в густом дыму и темноте.

• Если с вами летят дети, научите их, что они должны делать в чрезвычайной ситуации.

• Если вы знаете, где лежат средства спасения, легче будет их найти в хаосе чрезвычайного происшествия. Хотя такие инциденты редки, не мешает проверить, нет ли под креслом бомбы.

• Большинство авиакомпаний имеют специальные цветные инструкции, показывающие, как покинуть самолет в случае инцидента. Изучите эти инструкции. Опросы показали, что пассажиры всегда слишком заняты, чтобы прочитать инструкции, но все же найдите для этого время. Вы можете оказаться предоставленными самим себе и должны знать, что делать. Борт-проводники могут быть напуганы, как и другие.

• Когда посадка завершена и на борту есть свободные места, можно пересесть на более удобное место. Однако поторопитесь —

такой возможностью могут воспользоваться и другие. Будьте предупредительны и вежливы с бортпроводниками — они могут вам помочь занять более удобные места.

Недавний анализ показал, что число травм от предметов, упавших с багажных полок в самолете, растет. Чтобы снизить вероятность травм от упавшего багажа, помните следующее:

• избегайте мест под багажными полками, определите номера мест у прохода и попросите в кассе другое место;

• сдайте тяжелые вещи в багаж, возьмите на борт только легкие вещи;

• если вы увидели, что кто-то ставит на багажную полку очень тяжелые вещи, скажите бортпроводнику, чтобы убрали багаж.

4.3.3. Безопасность авиаперелета

Чтобы свести риск коммерческих полетов к минимуму, помните следующее:

• Летайте из крупных международных аэропортов. Небольшие региональные аэропорты в некоторых странах могут не соответствовать стандартам безопасности. Если вы выбрали для полета небольшой самолет, не летайте в плохую погоду (узнайте местный прогноз погоды) и ночью.

• В некоторых странах разрешено летать на военных самолетах. Будьте осторожны, особенно в регионах военных конфликтов или повышенной угрозы терроризма.

• Обратите внимание на предполетные сообщения экипажа и на расположение аварийных выходов.

• Если вам придется эвакуироваться из самолета, оставьте свою ручную кладь. Самое необходимое храните в кошельке-поясе и всегда держите при себе.

• Пристегивайте ремни безопасности, это защитит вас, если самолет попадет в зону турбулентности. Это происходит внезапно и может привести к серьезным травмам и к фатальному исходу даже во время нормального полета.

• Не пейте слишком много алкоголя в полете. Салоны авиалайнеров герметизированы, и алкоголь действует сильнее, чем на

уровне моря. Кроме того, обезвоживание организма, связанное с волнением по дороге в аэропорт и при прохождении контроля, также усиливает действие алкоголя. Сочетание обезвоживания, высоты и алкоголя может иметь серьезные последствия. Не переедайте. Это тоже может иметь отрицательные последствия в условиях полета.

• Если во время отпуска вы занимались глубоководными погружениями, постарайтесь не отправляться в полет ранее, чем через 24 часа после последнего погружения. Вы еще находитесь в состоянии декомпрессии, и требуется время для полного удаления из организма токсичных газов. Более детальную информацию можно получить в школе глубоководных погружений.

• Пожары на борту, к счастью, редки, но дым может быстро заполнить салон. Как в воздухе, так и на земле дым очень опасен, так как содержит токсичные вещества. Пробирайтесь к ближайшему аварийному выходу по меткам на полу и двигайтесь быстро. Это увеличит шансы на спасение. В продаже имеются специальные респираторы, снабженные системой фильтров, поглощающих токсические вещества. Относительно их использования ведутся споры, так как требуется время, чтобы их надеть, и это задерживает выход из самолета.

• Наденьте в полет одежду из натуральных тканей. Синтетические ткани более опасны, так как плавятся от огня. Натуральные ткани обеспечивают свободную циркуляцию воздуха, что предотвращает перегрев. Идеальны длинные рукава, так как лучше, если при пожаре кожа будет закрыта. Обувь тоже должна быть из натуральных материалов. Не носите туфли на высоких каблуках, так как они могут повредить эвакуационный трап.

• Последствия разгерметизации ощущаются через несколько секунд. В этом случае необходимо как можно быстрее надеть кислородную маску и активировать подачу кислорода. Сначала наденьте свою маску, потом можете помогать другим. Экипаж инструктирует, как пользоваться маской, до начала полета. Персонал не сможет помочь вам, так как они должны надеть свои маски.

• Надо знать, где находится ваш спасательный жилет и как им пользоваться. Сориентируйтесь, где находятся спасательные плоты и как их надувать. Другие плавсредства, такие как подушки кресел и пустые закрытые бутыли из-под воды, тоже могут быть полезны.

4.3.4. Безопасность полета на маленьких самолетах

В некоторых регионах маленькие самолеты — единственное транспортное средство, например, если вы отправляетесь на сафари или в дикие отдаленные места. Маленькие самолеты летают вне основных аэродромов и сами подвергаются специфическому риску.

Следующие рекомендации покажут, как этого избежать.

• На летном поле держитесь подальше от площадок, предназначенных для воздушных такси, и никогда не приближайтесь к самолету пешком или на машине без разрешения службы аэродрома. Не приближайтесь к движущимся самолетам.

• На летном поле держитесь подальше от самолетов, пропеллеров, лопастей винтов и реактивных двигателей. Минимальное безопасное расстояние от пропеллера составляет около 5 метров, от передней части реактивных двигателей — 25 м и от хвостовой части — 50 м. Шум аэродрома может ввести в заблуждение, особенно когда маневрируют сразу несколько самолетов. Пилоты воздушных такси не всегда видят, что происходит на поле вокруг самолета.

• Шум двигателей воздушного такси может повредить барабанные перепонки. Имеет смысл купить приспособление для защиты ушей.

• Следите за сохранностью вашего багажа, особенно ручной клади, на поле около самолета.

• Не курите на летном поле, особенно около самолета, вблизи топливных резервуаров и в ангарах.

4.3.5. Безопасность полета на вертолете

Вертолеты становятся все более популярным видом воздушного транспорта. Для организации экскурсий турфирмы регуляр-

но арендуют коммерческие вертолеты. Бизнесмены часто летают на деловые встречи на вертолетах. Однако вертолеты могут представлять большую опасность при неосторожном поведении, особенно их винты. Шум двигателя может заглушить шум хвостового винта.

Вот **основные правила поведения на вертолетной площадке.**

• Никогда не заходите на вертолетную площадку без разрешения соответствующих служб.

• Никогда не подходите к вертолету сзади. Пилот вас не видит, а хвостовой винт очень опасен. Вблизи вертолета всегда перемещайтесь впереди, где пилот вас видит.

• Не подходите к вертолету вниз по склону, а выйдя из вертолета, не поднимайтесь вверх по склону, чтобы не попасть под лопасти винта.

• Приближаясь к вертолету, установите контакт с пилотом, и если он подает сигналы, следуйте его указаниям.

• Если винты вращаются, не подходите к вертолету без разрешения пилота. Приближаясь к вертолету, наклоните голову, чтобы не попасть под лопасть винта. Если поле неровное, вероятность попасть под лопасть больше, поэтому убедитесь, что места для прохода достаточно, прежде чем идти. Если вы в этом сомневаетесь, оставайтесь на месте.

• Не входите и не выходите из вертолета без команды пилота. Проверьте, что весь ваш багаж, взятый на борт, в безопасности.

• Завихрения, создаваемые винтом, поднимают с земли всякий мусор, песок, стебли и листья растений. Вертолетная площадка должна поддерживаться в чистоте. Однако во время экскурсии вы можете приземлиться в неподготовленном месте. Во время приземления защитите глаза и проверьте, что ваш багаж в безопасности и что шляпа не улетит.

• Держите длинные предметы, такие как штативы, параллельно земле, чтобы не задеть винты.

• Пристегните пояс безопасности на все время полета. При полете над водным пространством наденьте спасательный жилет.

• Узнайте, можно ли поддерживать контакт с пилотом во время полета. Внимательно выслушайте предполетный инструктаж и поинтересуйтесь, как открыть дверь в случае чрезвычайной ситуации.

4.3.6. Самочувствие в полете

Реальная опасность — обезвоживание. Салоны самолетов имеют пониженную влажность, способствующую обезвоживанию, поэтому важно пить много воды. Избегайте алкоголя, чая и кофе, так как они усиливают обезвоживание.

Если вы страдаете респираторным заболеванием, проконсультируйтесь с врачом, можно ли вам летать. Если остались сомнения, обратитесь к турагенту, который свяжет вас с медицинским представителем авиакомпании.

Некоторым путешественникам трудно приспособиться к разнице во времени при перелете в другой часовой пояс. Ваши биологические часы могут "испытать сбой" при попытках работать, когда вы должны спать. Если вам предстоит серьезная встреча, прилетайте на несколько дней раньше, чтобы приспособиться к другому часовому поясу.

Если вы собираетесь лететь на запад, после 18 часов избегайте яркого света. При полете на восток избегайте яркого света до 10 часов утра.

Как считают некоторые эксперты, любая поездка, в которой пассажир должен сидеть в одном положении больше четырех часов — в автомобиле, в самолете или в поезде — повышает риск образования тромбов в сосудах ног.

Во всяком случае, пожилые люди или люди с заболеваниями сердечно-сосудистой системы, летящие на большие расстояния, подвергаются риску образования тромбов. Важно поддерживать в полете нормальную циркуляцию крови в ногах. Снимите обувь или наденьте удобные шлепанцы и регулярно двигайте ногами вверх и вниз либо прогуляйтесь по проходу.

Прибыв на место после длительного перелета, продолжайте упражнения. Это предотвратит отек ног, опасный для пожилых людей.

Простуда может вызвать проблемы с ушами или пазухами носа, так как изменение давления вызывает дискомфорт, и не удается выровнять давление во внутреннем ухе и внешнее давление. Попытайтесь продуть нос. Нужно избавиться от болезни до полета или проконсультироваться со своим врачом. Он может прописать курс лечения.

Если вы подвержены воздушной болезни, обратитесь к врачу, чтобы он прописал вам средство от воздушной болезни.

4.3.7. Угон самолета и стратегия выживания

За последние несколько десятилетий сложился сценарий угона. После захвата авиасудна террористы запугивают пассажиров и команду, производя страшный шум и угрожая оружием. Затем они направляются в кабину и сообщают пилоту об угоне. Пилот сообщает об этом пассажирам — это первое указание, что что-то происходит. Террористы сами рискуют, поэтому их поведение неразумно и быстро переходит в ярость.

Следующие рекомендации помогут вам не стать жертвой.

• На борту авиалайнера, угнанного террористом-смертником, вы подвергаетесь двойной опасности. Одна из них — со стороны террористов, другая — со стороны правительства, в воздушном пространстве которого вы находитесь. Оно может отдать приказ сбить самолет.

Если вы видите, что ничего не остается, кроме как действовать, действуйте быстро.

Попытайтесь получить поддержку других пассажиров и команды. Помните, что, если самолет вылетел из американского или европейского аэропорта, вряд ли у террористов есть огнестрельное оружие. Немедленно окажите сопротивление террористам.

• Если есть подозрение, что это обычный угон с изменением пункта назначения, не привлекайте к себе внимания и сохраняйте спокойствие. Если будете паниковать, то привлечете к себе внимание террористов. Успокойте своих попутчиков и помните, что в большинстве таких угонов пассажиры и команда не пострадали.

При таком угоне не надо пытаться обезвредить террористов. Они нервозны, напуганы и опасны. Они знают, что, если будут схвачены, им грозит долгий тюремный срок. Они доведены до отчаяния. Сам факт, что они совершили такие действия, означает, что они сознательно пошли на огромный риск.

• Если угонщики отдали вам какое-то приказание, подчинитесь, будьте вежливы, не вступайте в споры, сохраняйте чувство собственного достоинства, чтобы не привлекать к себе внимания.

• Не встречайтесь с террористом взглядом. Он может воспринять это как агрессию и брошенный ему вызов. Смотрите вниз; посмотрите на него, только если он этого потребует.

• Постарайтесь не давать информации о себе, особенно если работаете в государственных учреждениях.

• Возможно, что преступники соберут ваши паспорта. Вы можете привлечь их внимание, если откажетесь сдать паспорт. Пассажиров могут разделить на группы в зависимости от пола или национальности. Подчинитесь. Не пытайтесь прятать деньги и ценности, чтобы не привлекать внимания к себе.

• Для разрешения таких ситуаций требуется длительное время. Приготовьтесь к долгим испытаниям.

• Не пытайтесь вступать в контакт с террористами, даже если больны и испытываете дискомфорт. Лучше обратитесь к членам команды. Однако по мере развития событий вас может успокоить разговор с одним из террористов.

• Постарайтесь создать психологический портрет террористов. Некоторое время спустя вы поймете, кто из них лидер. Вы почувствуете, что некоторые более сговорчивы. Тогда подождите, когда кто-нибудь из них окажется рядом с вами, и заговорите с ним. Однако не пытайтесь просить для себя предпочтительного отношения.

• Обычно власти просят освободить женщин и детей в обмен на пищу и горючее. Ели вы путешествуете с семьей, есть шанс, что женщины, дети и пожилые люди будут освобождены в первую очередь.

• Обычно такие инциденты разрешаются, когда власти удовлетворят требования террористов освободить политзаключен-

ных или разрешат вылет в другой пункт. Спецназ привлекается только в исключительных случаях. Операции по освобождению заложников на авиалайнерах трудны и опасны, но могут оказаться успешными. Это зависит от многих факторов, таких, как конечный пункт полета, опыт участия военных и полицейских в такого рода операциях, и от самих террористов.

• При освобождении заложников первыми признаками начала операции могут быть громкие взрывы, шум, дым и крики, чтобы сбить с толку и отвлечь внимание террористов. Постарайтесь сжаться в комок. При возможности лягте на пол и не поднимайте головы, пока шум не стихнет.

• Если вы увидели за окном перемещения военных, ждите, что должно что-то произойти. Будьте к этому готовы.

• Если во время операции по освобождению заложников возникнет пожар, бегите к ближайшему аварийному выходу и покиньте самолет. Помните, дым токсичен и очень опасен.

• Террористы сначала будут растеряны и напуганы и сконцентрируют внимание на атакующих. Однако после первого шока они могут сосредоточиться на пассажирах. Здесь надо проявлять спокойствие и взаимопомощь, чтобы уменьшить риск.

• Если служба спасения приказала покинуть самолет, поторопитесь. Избегайте резких движений, которые могут быть истолкованы как угроза, поднимите руки над головой и кричите, что вы пассажир, чтобы вас не приняли за террориста. Соблюдайте указания полиции и военных.

• Обычно все покинувшие самолет находятся под подозрением, так как угонщики могут скрываться среди пассажиров, поэтому с вами могут сурово обходиться до установления личности.

4.4. Железная дорога. Метро

4.4.1. Безопасность на железной дороге

Для многих поездка за границу на поезде — это сильное искушение. Для кого-то это ностальгия по тем годам, когда поезд

был основным видом транспорта. Для других наземное путешествие более привлекательно в свете недавних авиакатастроф.

Действительно, поездка на поезде менее рискованна. Статистически это самый безопасный вид наземного транспорта. В последнее десятилетие шансы погибнуть или получить тяжелые травмы в автомобиле в 15 раз выше, чем на поезде.

Очевидно, что поездка на поезде по территории стран, где правительства не заботятся о соблюдении правил безопасности, сопряжена с риском.

Сеть железных дорог легкодоступна террористам. Здесь очень трудно им противостоять — железные дороги протянулись на многие тысячи километров, что делает практически невозможной их защиту.

Вокзалы

• Прежде чем приобретать билеты на поезд, узнайте, надежна ли железнодорожная система, которой вы собираетесь пользоваться. Во многих развивающихся странах грузовые и пассажирские поезда движутся по одним и тем же путям и может отсутствовать инфраструктура связи для точной координации движения. В некоторых странах, таких как Индия, крушения поездов происходят с пугающей частотой. Узнайте в посольстве данной страны о последних крушениях, террористических актах, преступлениях против пассажиров.

• Находясь в чужой стране, постарайтесь забронировать билеты заранее и приехать на вокзал задолго до отхода поезда. Во многих странах поезда могут быть опасно переполнены.

• По возможности расплачивайтесь местной валютой. Полезно знать немного язык, чтобы быстрее объясниться. Это создаст впечатление, что вы разбираетесь в обстановке, и отпугнет преступников.

• Проверьте, что кассир не взял с вас "специальную плату" за билет. Дополнительная плата, естественно, идет в карман кассира, зарплата которого очень низка. В некоторых развивающихся странах это обычная практика. Вам придется заплатить, ина-

че не получите билет или отстоите очередь в несколько сотен человек.

• На вокзале постарайтесь не привлекать к себе внимания вызывающей одеждой или поведением. Никогда не считайте, что как западный человек вы имеете преимущества. От вашего отношения к местным жителям зависит отношение к вам.

• Не забывайте, что среди ваших попутчиков могут быть члены местных криминальных структур. Вокзалы притягивают бандитов, а также обеспечивают террористам идеальное место для их акций. Будьте на вокзале предельно внимательны и постарайтесь не задерживаться там.

• Будьте осторожны с бесхозными свертками и багажом. Даже урны для мусора на вокзале могут служить взрывным устройством.

• Узнайте, где находятся запасные выходы, и хорошо изучите схему вокзала, чтобы быстро его покинуть при чрезвычайной ситуации. Не задерживайтесь вне здания вокзала. Террористы и преступники выбирают там себе жертву, если считают, что внутри их могут поймать. При поездке с группой держитесь все вместе и следите за детьми.

• Железнодорожные платформы могут быть переполнены, и люди под натиском толпы падают на пути. Не стойте на краю переполненной платформы, когда к ней приближается поезд, особенно если идет дождь и скользко. Подождите, когда поезд остановится.

• Стоять на краю платформы опасно и по другой причине. Поезда, не останавливающиеся на станции, движутся на большой скорости, и машинист не сможет остановиться, если кто-то упадет на пути. Следите за инструкциями на вокзальных табло. Они сообщают о приближении поездов и обеспечивают безопасность.

• Постарайтесь не ездить в одиночку. Во многих странах нет отдельных купе, и вы везде будете привлекать любопытные взгляды, особенно в очень бедных регионах. Остерегайтесь воришек. Если вас хотя бы двое, один может отдыхать, а другой — присматривать за вещами. Если даже вы едете в отдельном купе, не оставляйте

вещи без присмотра. Поезда тормозят и останавливаются, чтобы пропустить другой поезд или перейти на другой путь, и в это время в вагон могут проникнуть воры.

• В некоторых странах торговцы со своим товаром немедленно окружают остановившийся на станции поезд. Среди них могут быть воры, поэтому не высовывайтесь из окон с пачками наличных денег или кошельком, крепко держите фото- и видеоаппаратуру.

• Готовясь к поездке, подумайте, что делать, если поезд сломается в нескольких сотнях километров от ближайшего населенного пункта, в неизвестном месте чужой страны. Здесь, возможно, придется пробыть некоторое время, прежде чем придет подмога. Возьмите с собой достаточное количество воды и пищи на такой случай.

• В некоторых развивающихся странах нет платформ как таковых и пассажирам разрешено свободно расхаживать вдоль путей. Контактный рельс под высоким напряжением и проносящиеся мимо поезда делают ситуацию очень опасной. Придерживайтесь обозначенных мест и пешеходных переходов. Мокрые рельсы могут быть очень скользкими.

• Остерегайтесь попыток преступников сбить вас с толку, пока кто-то несет ваш багаж. Драки между местными, громкие споры, визг и другие отвлекающие факторы могут быть уловкой.

Поездка по железной дороге

Столкновения и пожары представляют большую опасность при поездке по железной дороге. Если произойдет крушение вашего поезда, вы можете получить тяжелые травмы или ожоги. Дизельные локомотивы наиболее подвержены пожарам, так как топливные баки при ударе могут быть повреждены.

При таких крушениях указания команды, если система связи с пассажирами работает, жизненно важны. Однако если вы не знаете местный язык, следуйте за другими людьми.

Проблема в том, что испуганные люди либо поддаются панике, либо цепенеют от страха. Вам придется принимать соб-

ственное решение. Здесь очень важны быстрота и осознание опасности.

Перед поездкой на поезде обратите внимание на следующее:

• У многих поездов имеется большой зазор между платформой и поездом. Многие пассажиры, особенно с тяжелым багажом, получали травмы при входе и выходе из поезда.

• При резком торможении поезда можно получить травмы от падающего багажа и других предметов. Если полки забиты тяжелым багажом, не сидите под ними или рядом. В спальных вагонах ставьте багаж в ящики под сиденья.

• На старых или содержащихся в плохом состоянии поездах не прислоняйтесь к дверям во время движения. Они могут самопроизвольно открыться.

• Не выходите из поезда до полной его остановки. Известны несчастные случаи, когда люди попадали между платформой и движущимся поездом.

• При поездках с маленькими детьми проверьте, что они хорошо устроены в своих переносных креслицах. Не держите ребенка на руках. Если поезд резко затормозит, вы полетите вперед и придавите его своей массой.

• Не высовывайте руки или голову из окна движущегося поезда. На многих железных дорогах поезда проходят близко друг к другу, и обычно очень маленькое пространство разделяет вагон и стенки туннеля.

• Можно подвергаться гораздо более высокому риску в первом вагоне поезда с двигателями, расположенными в хвостовой его части. В некоторых странах преобладают поезда такого типа. Если вам предстоит ехать в таком поезде, выбирайте место в хвостовом вагоне.

• В регионе с высоким уровнем преступности не ездите в пустых вагонах. Если пассажиры выходят на станциях и вагон постепенно пустеет, перейдите туда, где есть люди, особенно если вы одинокая женщина или путешествуете вдвоем с подругой.

• До начала поездки изучите путь к выходу. Многие поезда имеют автоматические скользящие двери или стандартные двери, открывающиеся посередине. Познакомьтесь с инструкцией по открыванию дверей, но помните, что при столкновении энергопитание может быть нарушено, и это не позволит открыть двери. Можно открыть их, потянув рычаг экстренного открывания.

• В некоторых странах в поездах над окнами висит маленький молоток, чтобы разбить стекло в чрезвычайной ситуации. Для этого ударьте по стеклу в углу окна. Однако иногда молотков нет или эта возможность не может быть использована в первую очередь.

• Сошедший с рельсов поезд может сильно наклониться, и может быть трудно разбить стекло. Если это удастся, то вас подстерегает другая опасность — падающие осколки стекла или необходимость вылезать в окно, усеянное по краю острыми осколками. Нужно удалить стекла из разбитого окна, чтобы не пораниться. Считается, что это одна из главных причин, по которой людям не удается быстро покинуть поезд после крушения.

• В любом случае нужно двигаться быстро. Неизвестно, повреждены ли топливные баки, создающие риск пожара. Оставьте свой багаж и скорее покиньте поезд, убедившись, что на соседнем пути нет поезда. Уйдите подальше от поезда, чтобы не получить ожогов в случае пожара. Если придется бежать вдоль путей, будьте осторожны и не наступайте на электрические кабели. Воздушные контактные кабели под напряжением 25 000 вольт могут упасть на землю или на пути.

• Не рассчитывайте на помощь персонала. Машинист может быть ранен или убит, а другие члены бригады, вероятно, попытаются покинуть поезд. Ориентируйтесь на то, что никто не придет вам на помощь. Позаботьтесь о себе сами, и когда ситуация стабилизируется, можете помочь другим.

4.4.2. Метро

В большинстве стран, имеющих метро, уровень безопасности высокий. Однако бывают и несчастные случаи. С большей вероят-

ностью можно стать жертвой преступников, орудующих на станциях или около них.

Очевидно, что на станциях метро, как на большинстве крупных транспортных узлов, преступники собираются потому, что имеющиеся здесь толпы людей представляют легкую добычу.

Для террористов метро также может быть привлекательной мишенью.

При поездках в метро соблюдайте следующие правила:

• Эскалаторы потенциально опасны, особенно на переполненных станциях. Будьте на эскалаторе внимательны, особенно если у вас тяжелый багаж.

• Хорошо завяжите шнурки на обуви, закройте молнии на одежде и уберите все висящие ремешки на рюкзаках и сумках — все это может попасть в движущиеся части эскалатора. Если с вами что-то произойдет, нажмите аварийную кнопку вверху или внизу эскалатора. Особую осторожность соблюдайте во время дождя, так как эскалатор может быть скользким.

• Попадая между поручнем и движущимися частями эскалатора, люди получали тяжелые травмы. По этой причине не бегите вверх и вниз по эскалатору, а идите медленно. Всегда стойте лицом по направлению движения эскалатора. Держитесь за поручень и крепко стойте на ногах.

• Будьте осторожны с бесхозными вещами — багажом, свертками и велосипедами. Известны случаи, когда террористы начиняли обычные вещи взрывчаткой.

• При покупке билета не забывайте о своих вещах. Пока вы опускаете монету в щель автомата, преступникам легко утащить оставленный без присмотра багаж и раствориться в толпе. Таким образом было украдено много портативных компьютеров.

• Не забывайте о своих вещах и в поезде. В тесноте вагонов карманники чувствуют себя вольготно. Мобильные телефоны, висящие на поясных ремнях, для них особенно привлекательная добыча.

• Попытайтесь найти сидячее место, прежде чем ухватиться за поручень. В случае инцидента сидеть безопаснее.

• Если поезд остановился в туннеле между станциями, прослушайте объявления машиниста. Обычно это кратковременная задержка, и поезд возобновит движение в течение нескольких минут.

• Если машинист объявит об эвакуации, не исключено, что придется открывать дверь вручную. Для этого следует воспользоваться приспособлением для экстренного открывания дверей. Читайте соответствующую инструкцию всякий раз, когда едете в метро. Это сохранит драгоценные секунды при несчастном случае.

Если машинист не дает указаний, эвакуируйтесь самостоятельно. Идите на свет ближайшей станции между рельсами, не касаясь их. Держитесь подальше от контактного рельса, расположенного обычно под платформой. Не бегите.

Если свет в конце туннеля не виден, то лучше остаться в поезде и переместиться к центру вагона. В большинстве метрополитенов предусмотрены специальные процедуры для вывода застрявших поездов.

• Если кто-то застрял в дверях или произошел другой опасный инцидент, воспользуйтесь стоп-краном. Если потянуть рычаг, поезд немедленно остановится.

• Постарайтесь не ездить в метро ночью. Но если это необходимо, не рекомендуется ездить в одиночку, особенно женщинам. Если ваш вагон опустел, перейдите на следующей станции в другой вагон, где есть люди.

• Избегайте ночью темных пустынных станций. Постарайтесь организовать свою поездку так, чтобы выйти на более людной и освещенной станции, менее привлекательной для криминальных элементов.

• Во многих процветающих городах, таких как Рим или Лондон, агрессивные попрошайки выпрашивают деньги у выглядящих доверчивыми людей. Чаще они пристают к женщинам. Если к вам подошли попрошайки, будьте тверды, но вежливы. Уйдите, если необходимо. Если они не отстают от вас, постарайтесь привлечь внимание других пассажиров. Когда вы видите несчастных людей, вы-

нужденных попрошайничать, и хотите дать им денег, не вынимайте кошелек, держите в кармане немного мелочи на этот случай.

• Перед поездкой в метро проверьте, не ожидается ли каких-нибудь крупных мероприятий, способных испортить вашу поездку. Классический пример — футбольные матчи. Переполненные станции — наименьшее зло. Пассажир может стать жертвой противостояния между двумя кланами болельщиков. Крупные политические демонстрации тоже могут вызвать проблемы. Если событие может привести к напряженности, избегайте станций, расположенных в месте его проведения.

4.5. Автомобильные дороги

4.5.1. Выбор автомобиля и подготовка к поездке

При аренде автомобиля за рубежом может оказаться, что правила аренды могут отличаться от принятых у вас дома. Шансы получить никуда не годный автомобиль могут быть велики. Кроме того, процедура получения водительских прав в западных странах обеспечивает высокий уровень большинства участников дорожного движения. Однако в некоторых регионах достаточно просто купить автомобиль.

Для поездки на автомобиле за границей нужно иметь международные водительские права (International Driving Licence) и страховку соответствующего уровня. Поставьте в известность своего страхового агента, что собираетесь водить автомобиль за границей, иначе вы можете лишиться возмещения.

Вот ***основные правила аренды автомобилей за рубежом.***

• Вступите в AA, RAC или местную страховую организацию. Вам нужны гарантии, что в случае ДТП вы можете рассчитывать на помощь. При поездках по Европе или развитым странам ваше членство в этих организациях может распространяться на возмещение расходов на их территории. Информируйте перед отъездом ваши страховые организации.

• Арендуйте автомобиль в международной компании. Такая компания имеет инфраструктуру, гарантирующую, что автомобиль

в хорошем состоянии и удовлетворяет стандартам безопасности страны, где вы будете ездить. Она также обеспечит страховую поддержку в случае, если вы окажетесь в трудной ситуации. Вас должны обеспечить инструкцией по управлению автомобилем, которую можно использовать для отыскания и устранения неполадок. В этом могут помочь турагент или администрация отеля.

• Не нанимайте автомобиль у незарегистрированных фирм, которые обещают слишком хорошие условия. Вы получите то, за что заплатите — дешевая сделка означает опасный автомобиль.

• Полезно записать регистрационный номер, модель и цвет. Если автомобиль украдут или если вы забудете, где его припарковали, то по крайней мере сможете дать описание.

• Выберите автомобиль, соответствующий местным условиям. Если регион неспокойный, лучше арендовать простой автомобиль неброского цвета, чтобы не привлекать внимания.

• Осмотрите автомобиль, начиная снаружи. Проверьте шины и убедитесь, что их протекторы подходят к ожидаемым дорожным условиям и что они хорошо надуты. Давление в шинах — важный фактор в ДТП. При движении масса автомобиля оказывает давление на шины. По рекомендации производителей при изменении температуры на 5 градусов давление в шинах нужно менять на 1 Па. Если вы собираетесь остаться в стране на некоторое время, то необходимо ежемесячно проверять давление, чтобы оно соответствовало рекомендации производителей. Помните: тяжело нагруженный автомобиль с плохо надутыми шинами сильно повышает вероятность ДТП.

• Проверьте все огни автомобиля: фары, указатели торможения и поворота. Они должны быть в полном порядке днем и ночью.

• Проверьте, нет ли повреждений на корпусе, и если обнаружите, укажите на это представителю фирмы, чтобы не расплачиваться за чужие ДТП. Если автомобиль был свежевыкрашен, это может быть попытка скрыть недавнее ДТП.

• Проверьте, чтобы двери, окна, багажник и капот хорошо запирались. В жарком климате предпочтительны автомобили с кон-

дицонером, чтобы не открывать окна. Двери также должны быть заперты.

• Убедитесь, что стеклоочистители исправны, в двигателе достаточно масла, а в радиаторе — воды и аккумуляторы заряжены.

• Узнайте потребление горючего и заправьте количество, необходимое для вашей поездки.

• Проверьте отделение для запасной шины, убедитесь, что она нужного размера и имеет хороший протектор. Проверьте, чтобы набор инструментов содержал домкрат, гаечный ключ нужного диаметра и предупредительный знак об аварии. Возьмите также небольшой ручной огнетушитель.

• Проверьте, что автомобиль имеет ремни безопасности и исправные гнезда их крепления. Проверьте также освещение салона. Убедитесь, что автомобиль функционирует нормально. Если имеется система тревожной сигнализации, проверьте ее и научитесь с нею обращаться.

4.5.2. Безопасное вождение

Езда на автомобиле в чужой стране может быть очень нервозной, особенно в регионах, где правила дорожного движения игнорируются и постоянно существует угроза ДТП.

Следующие рекомендации позволят снизить вероятность стать жертвой ДТП за рубежом:

• В некоторых странах быть за рулем очень опасно. В таком случае наймите автомобиль с водителем. Вы должны быть хозяином ситуации. Дайте понять, что будет дополнительная оплата за безопасное вождение. Но в случае ДТП предоставьте водителю свободу действий. Ваше вмешательство может только усугубить ситуацию.

• В некоторых странах арендованный автомобиль имеет специальные регистрационные наклейки. Нужно быть очень осторожным для предотвращения угона. Удалите такие наклейки, прежде чем садиться за руль. Наклейте их обратно перед возвращением автомобиля.

• Не садитесь за руль сразу после длительного перелета. Вы будете уставшим, и требуется размять ноги. Для некоторых садиться за руль в таком состоянии в незнакомом месте рискованно.

• Выберите автомобиль с боковыми зеркалами и зеркалом заднего вида и ездите на скорости, соответствующей дорожным условиям.

4.5.3. Железнодорожный переезд

При поездках на автомобиле вы наверняка встретитесь с железнодорожным переездом. Считается, что самый важный фактор — поведение водителей на переездах. Рассмотрим следующие правила:

• Приближаясь к переезду, смотрите и слушайте, не идет ли поезд. Ночью и в местах с плохой видимостью убедитесь, что в автомобиле нет отвлекающих звуков. Громкая музыка заглушит шум приближающегося поезда. Непосредственно перед пересечением путей, осмотритесь еще раз.

• Если автоматический шлагбаум опущен, не пытайтесь объехать его или ехать по путям. Обратите внимание на предупреждающие огни. В некоторых местах автоматические шлагбаумы действуют очень медленно, но спешка может оказаться гибельной.

• Там, где нет шлагбаума, убедитесь, что путь свободен. В некоторых местах приходится пересекать много путей. Если вы не уверены в себе, подождите, пока пройдет поезд.

• При переезде выберите подходящую скорость. Постарайтесь не менять передачи, чтобы не застрять.

• Если автомобиль застрял на переезде, все пассажиры должны немедленно его покинуть и уйти с путей. Если есть система тревоги или аварийный телефон, попытайтесь связаться с железнодорожниками. Если есть мобильный телефон, срочно позвоните в службу спасения. Если по какой-то причине автомобиль стоит на путях и приближается поезд, выйдите из автомобиля и быстро бегите от путей. Если поезд столкнется с вашим автомобилем, он может отбросить его в сторону или протащить вперед.

• Помните, что в зависимости от погодных условий тормозное расстояние товарного или пассажирского поезда до полной остановки составляет до двух километров.

4.5.4. Безопасность на дорогах

Криминальные банды и террористические организации редко подвергают себя напрасному риску и тщательно выбирают свою жертву. Они предпочитают слабых и доверчивых. Старайтесь выглядеть уверенным в себе и за рулем, чтобы создать у этих людей впечатление, что с вами лучше не связываться, и пусть поищут себе другую жертву.

• При поездке в опасные регионы следите за тем, что происходит вокруг вас. Это поможет избежать инцидентов. Будьте особенно внимательны в медленно движущемся потоке машин или перед светофором.

• Сделайте запасные ключи к автомобилю и всегда носите их при себе в поясном кошельке или даже бумажнике.

• Ваше поведение за рулем или на пассажирском сиденье дает сигнал водителям и пешеходам.

Если вы выглядите нервным, беспокойным, неуверенным в себе, окружающие сразу это поймут. Если у вас к тому же вид состоятельного человека, это еще сильнее привлечет к вам внимание преступных элементов. Не держите на виду ценные вещи. Демонстрируйте уверенность в себе, чтобы уменьшить шансы стать жертвой.

• Выработайте у себя привычку запирать двери и окна, находясь за рулем. Если вы застряли в пробке, никогда не открывайте окно, чтобы поговорить с уличными торговцами или мойщиками стекол. В неспокойных регионах не открывайте окно, чтобы спросить дорогу.

• Прежде чем сесть за руль, узнайте, какие части города наиболее опасны, и избегайте их. Имейте при себе карту города и, если вам нужно ее посмотреть, держите ее ниже уровня щитка управления, чтобы посторонние не видели, что вы не знакомы с местом. Оберните карту газетой, чтобы скрыть ее от любопытных глаз пе-

шеходов и незаметно пользоваться ею. Если заблудитесь, езжайте в ближайшее безопасное место, прежде чем взять в руки карту. Выходя из машины, не оставляйте карту на щитке управления или на сиденьи.

• Спланируйте свой маршрут заранее, записав номера дорог, названия улиц и перекрестков, и отмечайте, когда их проехали.

• Если вы наняли водителя, не отвлекайте его. Не заводите с ним разговоры на религиозные и политические темы. Не читайте на переднем сиденье газету или журнал, так как водитель невольно будет бросать взгляд на заголовки.

• Оставаясь в стране на длительный срок, узнайте места автомобильных пробок и часы пик и воздерживайтесь от поездок в это время. Найдите на автомобильном приемнике волну местной радиостанции, где сообщается о ситуации на дорогах.

• По возможности избегайте поездок по ночам и в плохую погоду. В сырую погоду, в тумане, на обледенелой дороге это вдвойне опасно, если вы не знакомы с местностью и пытаетесь найти дорогу.

• В местах большого скопления туристов старайтесь не проезжать мимо баров и клубов после их закрытия. В это время на дороге будет много водителей в состоянии алкогольного или наркотического опьянения. Здесь будут люди из разных стран с различными правилами и культурой вождения, что не способствует безопасности движения.

• Никогда не пейте и не принимайте наркотики за рулем.

• Пользуйтесь обычными противоугонными средствами, такими, как блокировка колес и тревожная сигнализация. Если угонщику придется разблокировать колеса или отключать сигнализацию, он дольше будет подвергаться риску быть пойманным, и это может его остановить. Он лучше поищет машину без противоугонных устройств.

• Паркуйте автомобиль так, чтобы колеса были повернуты к краю тротуара. Тогда его будет труднее отбуксировать. Не оставляйте на виду вещи, уберите их в багажник. Не оставляйте регистрационные документы на машину.

• Отлучаясь "на минутку" в магазин или гараж, не оставляйте двигатель включенным. Знающему свое дело вору достаточно одной-двух минут, чтобы угнать автомобиль. В таком случае страховая компания откажется выплатить возмещение, так как это ваша вина.

• Путешественники попадают в поле зрения преступников на АЗС, когда останавливаются заправить автомобиль топливом или просто отдохнуть. Посмотрите, не привлекаете ли вы чье-либо чрезмерное внимание. Останавливайтесь на АЗС, где есть другие автомобили, и старайтесь не привлекать внимания. Даже если вы устали, не съезжайте с дороги, чтобы поспать. Езжайте до следующей АЗС или до города.

• Если у вас возникло подозрение, что кто-то вас преследует, постарайтесь сделать несколько кругов, чтобы понять, есть ли за вами слежка. Если ваше подозрение подтвердится, поезжайте в ближайший полицейский участок или крупный отель, где вам помогут.

• Часто преступники притворяются пострадавшими водителями или пешеходами, чтобы обмануть доверчивого водителя. Они голосуют на дороге и, если машина остановится, отбирают ценные вещи и угоняют автомобиль. Никогда не останавливайтесь, чтобы оказать помощь, каким бы серьезным ни выглядел инцидент.

Если у вас есть мобильный телефон, вызовите необходимые службы или доезжайте до ближайшего города и сообщите в полицию и скорую помощь.

Есть и другие уловки. Например, преступники кладут на дорогу острые предметы, чтобы проколоть шины ничего не подозревающему водителю, а затем предлагают помощь в замене шины.

• Не подбирайте путешествующих автостопом или незнакомцев, попавших в беду. Будьте осторожны с одинокими полицейскими, останавливающими вас на дороге. Известно много случаев, когда лжеполицейские останавливали ничего не подозревающих водителей и грабили их. Если у вас есть сомнения, поезжайте до ближайшего города или ждите, пока вы не попадете в поток автомобилей, прежде чем остановиться.

• Классический прием — ударить в бампер арендованного автомобиля. Цель преступника — выманить вас из машины для осмотра повреждений. На вас тут же нападут, ограбят и, возможно, угонят машину. Если ваш автомобиль ударили сзади, не останавливайтесь, езжайте до ближайшего полицейского участка и обратитесь за помощью.

• При остановке перед светофором или в месте объезда дорожных работ следите за окружающей ситуацией. Не останавливайтесь в темных или пустынных местах.

• Если вы чувствуете себя незащищенным, особенно если вы женщина, положите муляж оружия на сиденье.

• Если на вас напали в вашем автомобиле, нажмите на кнопку сигнала и не отпускайте ее. Поезжайте в ближайшее безопасное место.

Если вас заставляют остановиться и не дают вести машину, не сопротивляйтесь и не вступайте в перебранку с налетчиками. Не делайте резких движений, держите руки так, чтобы они могли их видеть. Преступники сами рискуют и могут сорваться.

• В некоторых странах дорожные разборки стали серьезной проблемой. Часто такие инциденты заканчиваются перестрелкой по самым ничтожным причинам. Если вы стали свидетелем такого инцидента, не останавливайтесь, а поезжайте к ближайшему полицейскому участку.

• При поездке на большое расстояние купите запасную канистру топлива.

• Полезно иметь запасное оборудование на случай поломки. Бесценен мобильный телефон с номерами служб спасения. Нужны также фонарь, запасные шины, пища и вода и теплая одежда.

• Если ваш автомобиль сломался в неспокойном регионе, нужно съехать на обочину, снять и спрятать все ценные вещи и только потом попытаться вызвать помощь. Спросите название фирмы и имена людей, которые приедут к вам на помощь. Если вы решили остаться в автомобиле, не открывайте дверь, пока не убедитесь, что перед вами человек, прибывший к вам на помощь.

• Если шина спустилась в опасном месте, не останавливайтесь. Продолжайте медленно ехать на спущенной шине до безопасного места, прежде чем остановиться.

• При поездке в опасном регионе узнайте места, где лучше не появляться. Затем узнайте безопасные места на вашем маршруте. Если что-то случится, вы будете знать, куда ехать.

• Не останавливайтесь около храмов, среди толпы или у баров и клубов незадолго до их закрытия. Здесь быстро разгораются страсти, поэтому держите двигатель включенным и будьте начеку.

4.5.5. Угон автомобилей

Нападения на водителей в целях угона автомобиля совершаются все чаще в разных регионах мира, включая курортные зоны. Угонщики используют против своих жертв силу и оружие. Они могут быть одиночками или членами организованной преступной сети, специализирующейся на угоне автомобилей определенных марок, или преступниками, пытающимися скрыться от полиции после совершения какого-то преступления. Помните следующие правила:

• машину легче всего угнать около светофора или на главных перекрестках, где вы должны остановиться. Стоянки АЗС и супермаркетов — также рискованные места для угона. Никогда не оставляйте в машине ключи зажигания, даже на минуту, чтобы расплатиться за бензин;

• выйдя из машины или возвращаясь к ней, будьте начеку. Подходя к машине, оглянитесь вокруг и, если у вас возникли какие-либо подозрения, уйдите с парковки и позовите кого-нибудь на помощь, прежде чем открывать дверь автомобиля;

Если вы увидели, скажем, группу мужчин, направляющихся к вам, быстро садитесь в машину, заприте дверь и уезжайте со стоянки.

• если вы остановились у светофора или в потоке машин в уличной пробке, помните, что уличные торговцы, люди, спрашивающие дорогу или распространяющие листовки, могут быть потенциальными угонщиками;

• если угонщики вооружены, отдайте им автомобиль. Он застрахован, и вы можете купить другой. Ваша жизнь дороже автомобиля. Запомните приметы угонщиков: одежду, возраст, цвет волос и глаз и другие отличительные черты. Покиньте как можно быстрее место угона и сообщите об инциденте властям;

• если вы решили совершить поездку по опасной территории или планируете ехать ночью, скооперируйтесь с другим водителем. Тогда в случае поломки или несчастного случая, когда требуется оставить машину, у вас по крайней мере будет другой автомобиль.

4.5.6. Блокпосты и контрольно-пропускные пункты

На неспокойных территориях могут часто попадаться блокпосты и контрольно-пропускные пункты (КПП), и надо знать, как себя вести, приближаясь к ним. *Вот основные правила.*

• При поездках на автомобиле в неспокойных регионах будьте готовы встретить на дороге блокпост. Если вы уже пробыли на этой территории некоторое время, то будете интуитивно ощущать приближение к ним. Однако блокпосты могут быть развернуты очень быстро и располагаться в местах, совершенно неожиданных для водителей.

Ночью может быть трудно заметить блокпост на дороге, но, если люди в военной форме или полицейский патруль подают вам сигнал остановиться, следует подчиниться, даже если вы знаете, что у вас будут вымогать деньги. Нередко солдаты и полицейские открывали огонь по автомобилю только потому, что он не остановился на их блокпосту.

• В некоторых странах нужно знать, как приблизиться к военному или полицейскому КПП. Например, в Северной Ирландии на подъезде к КПП водители должны сбавить скорость и выключить огни. Считается, что фары будут освещать солдат, и они могут стать жертвой снайпера.

• Независимо от того, где вы находитесь и кто вас останавливает, не сопротивляйтесь и делайте то, что вам прикажут. Неподчинение может привести к неприятностям. Помните, что во многих регионах вам все равно придется заплатить, иначе вы окажетесь в

местной тюрьме по сфабрикованному приговору. Солдата или полицейского на КПП удовлетворит меньшая сумма, чем их начальника. Если вы будете арестованы, вам придется заплатить большую сумму, чем на КПП.

• Если вас остановили на КПП вооруженные солдаты, полицейские или даже боевики, ведите себя спокойно. Не делайте резких движений, не вступайте с ними в полемику. Будьте тверды, но вежливы и сохраняйте чувство собственного достоинства. Держитесь уверенно, и у вас будет меньше риска попасть в беду.

4.5.7. Безопасность поездки на мотоцикле

До 75% несчастных случаев с мотоциклистами связаны с другими транспортными средствами, обычно автомобилями. В остальных 25% несчастных случаев мотоцикл выходит из-под контроля и врезается в какой-нибудь объект у дороги. Часто причиной этого является прокол шины.

Обратите внимание на следующие рекомендации, и вы снизите риск несчастного случая при поездке на мотоцикле за границей.

• Если вы собираетесь погонять на мотоцикле в зарубежной поездке, застрахуйтесь. Предупредите страхового агента. Если вы этого не сделаете, то можете разориться, так как оплата медицинских услуг очень высока.

• Арендуйте мотоцикл у фирмы с надежной репутацией.

• Прежде чем арендовать мотоцикл, проведите беглый осмотр его дорожных качеств. Проверьте, чтобы в обеих шинах было надлежащее давление, так как виной многих несчастных случаев являются шины. Попросите инструкцию для пользователя. Если вы собираетесь возить пассажиров, может потребоваться отрегулировать давление в шинах на 10%.

• Убедитесь, что передние фары, указатели поворота и торможения исправны. Проверьте наличие тормозной жидкости и масла. Иногда трудно определить уровень масла в холодном двигателе, поэтому запустите его, чтобы сделать точный отсчет.

• Убедитесь, что измеритель топлива, если таковой имеется, функционирует и что в баке достаточно топлива для вашей поездки. Поинтересуйтесь расходом топлива — на какое расстояние можно уехать с полным баком. Помните, что при быстрой езде или на пересеченной местности требуется больше топлива.

• Осмотрите мотоцикл на предмет повреждений. Не исключено, что на нем ездили байкеры, а многие из них попадают в ДТП. Если у мотоцикла есть повреждения, попросите другую машину.

• При езде на мотоцикле к несчастным случаям могут привести многие факторы. Иногда отдыхающие садятся за руль, не умея ездить на мотоцикле.

• Большинство травм происходит не тогда, когда вы упали с мотоцикла, а когда вы ударились обо что-то твердое или попали между мотоциклом и дорогой или автомобилем. Если вам не удалось стать байкером или вы чуть было во что-то не врезались, откажитесь от гонок на мотоцикле.

• Алкоголь — одна из главных причин фатальных исходов при езде на мотоцикле. Он ослабляет внимание, и, если мотоцикл выйдет из-под контроля, водителю не поздоровится.

• Инциденты в городах объясняются тем, что часто водители автомобилей не видят мотоциклистов. Наденьте бросающуюся в глаза одежду.

• Высокая скорость — главная причина аварий мотоциклов, особенно на второстепенных дорогах с двухполосным движением. Постоянно думайте: "Если сейчас что-то случится, удастся ли мне избежать аварии?"

• Кожаная куртка или другая подходящая одежда обеспечит некоторую защиту при падении с мотоцикла, и очень полезен шлем. На многих курортах можно видеть мотоциклистов, гоняющих без шлема, в шортах и майке. Такое легкомыслие очень опасно.

• Статистика показывает, что для тех, кто ездит на мотоцикле нерегулярно, наиболее опасны первые 8 км.

• Песок, гравий и масляные пятна на полотне дороги ухудшают дорожные условия и могут быть причиной аварии.

4.5.8. Поездка на автобусе

При поездке на автобусе вы вверяете свою жизнь компании, которой принадлежит автобус, и водителю. В некоторых странах пассажирские автобусы не оснащены ремнями безопасности, поэтому пассажиры реально рискуют получить серьезные травмы.

В автобусе вы не защищены от преступников и террористов. Такие группы промышляют на популярных туристических маршрутах и в некоторых регионах захватывают автобусы и грабят пассажиров.

Следуя приведенным ниже рекомендациям, вы снизите риск при поездке на автобусе.

• Пользуйтесь автобусами известных и надежных операторов. Если вы выбрали дешевую компанию, то неизбежно окажетесь в разбитой машине. Ваш турагент даст вам информацию о надежных автобусных фирмах.

• Проверьте маршрут автобуса. Если он опасен, постарайтесь найти менее опасный маршрут. В некоторых странах не рекомендуется ездить наземным транспортом, гораздо безопаснее летать. Узнайте, были ли случаи нападения на автобусы, и если были, — когда имел место последний инцидент и каковы его мотивы.

• Не ездите на автобусе в периоды обострения напряженности и по ночам. Если вы отправляетесь в поездку на автобусе, сообщите кому-нибудь, когда выезжаете и когда должны прибыть на место.

• Выбирайте автобусы с ремнями безопасности или другими приспособлениями и пользуйтесь ими. При столкновении или резком торможении вы менее рискуете получить тяжелые травмы.

• Узнайте, где находится аварийный выход, и изучите, как открывается дверь. При столкновении для быстрого выхода из автобуса могут служить окна.

• Если у вас есть мягкий багаж, положите его перед собой напротив переднего кресла. Это уменьшит силу удара при столкновении.

• При столкновении пассажиры полетят вперед. Полезно принять "аварийную позу", подтянув колени к груди и положив на них голову. Если вы сильно сгруппируетесь, это может предотвратить падение из окна автобуса при столкновении. Около половины смертельных исходов происходит по этой причине.

• Не ставьте тяжелый багаж на верхнюю полку и не заставляйте проход крупными вещами.

• В некоторых странах пассажиры ездят на крыше автобуса. Не делайте этого. При повороте на верхнюю часть может действовать значительная центробежная сила и вам будет трудно удержаться.

• Не высовывайте голову и руки из окна.

• В некоторых странах террористы выбирают автобусы в качестве своей мишени. Увидев в автобусе бесхозные сумки и свертки, сообщите об этом водителю и не притрагивайтесь к ним.

• Следите за своим багажом. Убедитесь, что он помещен в багажный отсек. Ручную кладь постоянно держите при себе. В некоторых местах нельзя спать в автобусе, так как в это время вор может обчистить ваши карманы.

• Не возите в своем багаже горючие, токсичные и другие опасные вещества. При столкновении эти вещества могут привести к пожару.

• Если вы путешествуете в одиночку по опасной территории, возьмите с собой книги или журналы. Если вы будете читать во время поездки, это защитит вас от нежелательных собеседников и потенциального конфликта. В таких регионах старайтесь не встречаться ни с кем взглядом. За этим может последовать вопрос, что может втянуть вас в разговор, и т. д.

• Выйдя из автобуса, соблюдайте осторожность при переходе улицы. В некоторых регионах автобусы движутся по специальной полосе против основного потока уличного движения.

• Выйдя из автобуса, дождитесь сигнала водителя, прежде чем переходить улицу, и следите за уличным движением. Если припаркованный автомобиль или другое препятствие загораживает поле зрения, перейдите туда, откуда хорошо виден поток машин. Стойте подальше от задних колес автобуса, так как там находятся "слепые пятна", где водитель вас не видит. Если вы должны идти по дороге без тротуара, идите навстречу движению. Тогда вы сможете увернуться от приближающегося автомобиля.

4.5.9. Безопасность поездки в микроавтобусе

Во многих регионах мира микроавтобус — широко распространенный и популярный вид транспорта. Некоторые микроавтобусы могут потерять устойчивость, двигаясь на большой скорости, особенно при крутом повороте.

Запомните следующие рекомендации.

• Выберите надежную фирму или микроавтобус, предоставленный вашим отелем. Такие машины всегда в хорошем рабочем состоянии. Однако часто водитель ответственен за обеспечение безопасности. Понаблюдайте за поведением водителя и, если вы в нем не уверены, спросите его о техническом состоянии машины.

• Выбирайте микроавтобус с сиденьями, обращенными по ходу движения. При столкновении такие сиденья менее опасны. Если у них высокие спинки и диагональные пояса безопасности, они более надежны.

• В некоторых туристических зонах багаж ставят в задней части микроавтобуса, иногда просто сваливая вещи в кучу на последнее сиденье. Обычно этот багаж небезопасен, и при столкновении или резком торможении он может пролететь вперед, задеть пассажиров и поранить их. Потребуйте, чтобы багаж был закреплен.

• Узнайте, где находятся аварийные выходы и как действует механизм аварийного открывания дверей.

• Не оставляйте в проходе багаж и свертки, чтобы они не мешали пассажирам. Проверьте, чтобы аварийный выход не был загроможден.

• При поездке по неспокойной территории оденьтесь скромно, не носите дорогих часов (даже их имитации) и украшений. Это может привлечь нежелательное внимание и привести к неприятностям. Старайтесь по возможности стушеваться.

• Уважайте местные обычаи и ведите себя соответственно. Осознавайте себя обычным пассажиром. В общественном транспорте вы находитесь за пределами туристической зоны и отеля, и от вас вправе ожидать другого поведения.

• Определитесь, где вы находитесь, особенно при поездках по неспокойным территориям. Если автобус будет остановлен, например, на блокпосту, то, зная где вы находитесь, вы по крайней мере сможете самостоятельно добраться до ближайшего безопасного места.

4.5.10. Поездка в такси

Прибыв в пункт назначения, вы прежде всего хотите добраться до отеля и освежиться. Поэтому вы направляетесь к стоянке такси и берете первую попавшуюся машину. Такая манера поведения известна ошивающимся у транспортных узлов преступным элементам, и многие туристы становятся их жертвами через несколько минут после отъезда от терминала аэропорта.

Помните, что, садясь в такси, вы отдаете себя в руки чужого незнакомого человека.

• По прибытии в аэропорт остерегайтесь тех, кто предлагает поймать вам такси. Это закончится поездкой в разбитой машине и оплатой посреднику и водителю. Так действуют многие преступные группы, и беззащитного путешественника захватят и ограбят.

• Если такси вызывает у вас подозрение, подойдите к бюро заказа такси в здании аэропорта и наймите такси там, даже если ждать придется немного дольше. На стоянке такси вы скорее всего сядете в первую подошедшую машину. Когда водитель увидит состоятельного туриста, он может запросить высокую цену или ввести дополнительную оплату. Чтобы этого не случилось, узнайте все в бюро заказа такси.

• Если, поселившись в отеле, вы захотите пройтись, сначала подумайте, как вы будете возвращаться обратно, особенно ночью после выпивки. Узнайте телефон надежной службы такси у портье или турагента. Звонок будет принят, и фирма передаст заказ своим водителям. Если вы не можете дозвониться по данному вам номеру, попытайтесь обратиться в ближайший большой отель.

• Заказывая такси, не называйте свое настоящее имя, но не забудьте спросить имя водителя. Когда подъедет такси, спросите имя водителя как пароль. При заказе такси следите, чтобы никто вас не подслушивал. Если услышат, куда вы собираетесь ехать, или даже ваше имя, вы уже не будете в безопасности.

• Прежде чем садиться в машину, убедитесь, что у нее есть счетчик. Если он отсутствует, договоритесь о цене и следите, чтобы вас привезли туда, куда надо. Если водитель говорит, что счетчик сломан, и просит очень высокую плату, не садитесь в машину.

• Старайтесь не ездить в такси в одиночку и не разрешайте водителю останавливаться и подбирать кого-нибудь на улице. Это известная криминальная уловка. Водитель говорит, что ему надо подобрать родственника или другого таксиста, а потом они вместе грабят пассажира.

• Если водитель говорит, что барахлит двигатель и надо остановиться, будьте начеку. Настаивайте, чтобы он доехал до ближайшего безопасного места. Если такси сломалось, заставьте водителя вызвать другую машину. Оставайтесь в машине с закрытыми окнами и дверями и не открывайте их, пока не убедитесь в полной безопасности.

• Если вы не знаете местного языка, напишите адрес поездки на бумажке. Постоянно держите в кармане визитку или буклет отеля.

• Отметьте на карте достопримечательности вдоль вашего маршрута. У таксиста может создаться впечатление, что вы знаете местность, и он не будет отклоняться от короткого пути.

• Если вы часто пользуетесь услугами какой-то службы такси и вам нравится их обслуживание, дайте водителю чаевые. Если у вас будет репутация щедрого пассажира, то вас будут хорошо обслуживать.

• В некоторых странах многие таксисты предложат вам поехать на базар, где у их родственника собственная лавка и вам будут предоставлены специальные цены. С большой вероятностью вы потеряете время и наживете неприятности. Потребуйте, чтобы вас сразу везли туда, куда вам надо.

Список использованной и рекомендованной литературы

1. *Авдийский, В.И.* Теневая экономика и экономическая безопасность государства: Учебное пособие [Текст] / В.И. Авдийский, В.А. Дадалко, Н.Г. Синявский. М., 2017.

2. *Акимов, В.А.* Безопасность России. Национальная и международная безопасность [Текст] / В.А. Акимов, В.А. Баришполец, Н.А. Махутов, М.И. Фалеев. М., 2012.

3. *Арбатов, А.А.* Экономическая безопасность России: Общий курс: Учебник [Текст] / А.А. Арбатов. М., 2009.

4. *Артемьев, В.Р.* Информационно-коммерческая безопасность предпринимательской деятельности [Текст] / В.Р. Артемьев, Н.Н. Куняев. М., 2015.

5. *Баяндин, Н.И.* Технология безопасности бизнеса: Введение в конкурентную разведку: Учебно-практическое пособие [Текст] / Н.И. Баяндин. М., 2002.

6. Безопасность России. Правовые, социально-экономические и научно-технические аспекты [Текст]. Т. 2. Безопасность и защищенность критически важных объектов. В 2 ч. Ч. 1. М., 2012.

7. Бизнес — Безопасность — Телекоммуникации: Терминологический словарь [Текст]. М., 2011.

8. *Велесов, В.С.* Приемы самообороны [Текст] / В.С. Велесов. М., 2001.

9. *Вильчур, Н.Н.* Полицейские проверки бизнеса. 72 практических совета по прохождению [Текст] / Н.Н. Вильчур. М., 2015.

10. *Гасанов, Р.М.* Шпионаж и бизнес [Текст] / Р.М. Гасанов. М., 2009.

11. *Гладкий, А.В.* Бизнес-безопасность в современной России [Текст] / А.В. Гладкий. М., 2012.

12. *Гостюшин, А.В.* Энциклопедия экстремальных ситуаций [Текст] / А.В. Гостюшин. М., 2012.

13. *Деружинский, В.А.* Основы коммерческой тайны: Практическое пособие для предпринимателя [Текст] / В.А. Деружинский, В.В. Деружинский. Минск, 2015.

14. *Доронин, А.И.* Бизнес-разведка [Текст] / А.И. Доронин. М., 2010.

15. *Доронин, А.И.* Основы экономической разведки и контрразведки [Текст] / А.И. Доронин. Тула, 2009.

16. *Доронин, А.И.* Разведывательное и контрразведывательное обеспечение финансово-хозяйственной деятельности предприятия [Текст] / А.И. Доронин. Тула, 2011.

17. *Дэвис, Б.* Энциклопедия выживания и спасения [Текст] / Б. Дэвис. М., 2008.

18. *Землянов, В.М.* Своя контрразведка: Практическое пособие [Текст] / В.М. Землянов. Минск, 2013.

19. *Ильичев, А.А.* Большая энциклопедия городского выживания [Текст] / А.А. Ильичев. М., 2012.

20. Информация: поиск, анализ, защита [Текст] / Авт.-сост. И.Н. Кузнецов. Изд. 2-е. Минск, 2004.

21. *Камерон, Н.* Полное руководство по безопасности в загранпоездке [Текст] / Н. Камерон. М., 2014.

22. *Коледа, С.* Выживание [Текст] / С. Коледа. Минск, 2009.

23. *Криворотов, В.В.* Экономическая безопасность государства и регионов: Учебное пособие для студентов вузов [Текст] / В.В. Криворотов, А.В. Калина, Н.Д. Эриашвили. М., 2012.

24. *Максимов, С.Н.* Экономическая безопасность России: системно-правовое исследование [Текст] / С.Н. Максимов. М., 2008.

25. *Кузнецова, Е.И.* Экономическая безопасность и конкурентоспособность. Формирование экономической стратегии государства [Текст] / Е.И. Кузнецова. М., 2012.

26. *Куняев, Н.Н.* Правовое обеспечение национальных интересов Российской Федерации в информационной сфере [Текст] / Н.Н. Куняев. М., 2013.

27. *Ларичев, А.В.* Как уберечься от мошенничества в сфере бизнеса: Практическое пособие [Текст] / А.В. Ларичев. М.,2010.

28. *Лекарев, С.В.* Бизнес и безопасность от А до Я: Толковый терминологический словарь [Текст] / С.В. Лекарев, В.А. Порк. М., 2005.

29. *Мангушев, Д.Ф.* Бизнес и безопасность в России. Практическое пособие для малого, среднего и крупного бизнеса [Текст] / Д.Ф. Мангушев, И.А. Янышев, Д.А. Иванов, С. В. Колпаков. М., 2011.

30. *Мелтон, Кит.* Искусство шпионажа. Тайная история спецтехники ЦРУ [Текст] / Кит Мелтон, Роберт Уоллес , Генри Шлезингер. М., 2015.

31. *Минин, И.В.* Защита конфиденциальной информации при электронном документообороте [Текст] / И.В. Минин, О.В. Минин. М., 2010.

32. *Михайлов, Ю.Б.* Пожарная безопасность в офисе [Текст] / Ю.Б. Михайлов. М., 2013.

33. *Михайлов, Ю.Б.* Научно-методические основы обеспечения безопасности защищаемых объектов[Текст] / Ю.Б. Михайлов. М., 2015.

34. Мошенничество в платежной сфере. Бизнес-энциклопедия [Текст]. М., 2016.

35. *Плэтт, В.* Стратегическая разведка: Основные принципы [Текст] / В. Плэтт. М., 1997.

36. *Ронин, Р.* Своя разведка: способы вербовки агентуры, методы проникновения в психику, форсированное воздействие на личность, технические средства скрытого наблюдения и съема информации: Практическое пособие [Текст] / Р. Ронин. Минск, 2015.

37. *Соловьев, Э.Я.* Коммерческая тайна и ее защита [Текст] / Э. Я. Соловьев. М., 2011.

38. *Тарас, А.Е.* Безопасность бизнесмена и бизнеса: Практическое пособие [Текст] / А.Е. Тарас. М., 2012.

39. Технические средства, применяемые в охранной деятельности: Учебное пособие [Текст]. М., 2014.

40. *Ужегов, Г.Н.* Секреты выживания в чрезвычайных ситуациях [Текст] / Г.Н. Ужегов. М., 2014.

41. *Черкасов, В.Н.* Компьютерная преступность и ее предупреждение [Текст] / В. Н. Черкасов. Минск, 2015.

42. *Шабалин, В.Г.* Сделки с недвижимостью. Защита от криминала и недобросовестных партнеров [Текст] / В.Г. Шабалин, И.А. Смирнов, А.К. Кузьмина. М., 2016.

43. *Эриашвили, Н.Д.* Экономическая безопасность: Учебное пособие для студентов вузов [Текст] / В.А. Богомолов, Н.Д. Эриашвили, Е.Н. Барикаев; Под ред. В.А. Богомолова. М., 2010.

44. *Яковлев, В.А.* Шпионские и антишпионские штучки. [Текст] / В.А. Яковлев. М., 2015.

45. *Ярочкин, В.И.* Корпоративная разведка [Текст] / В.И. Ярочкин, Я.В. Бузанова. М., 2011.

46. *Ярочкин, В.И.* Словарь терминов и определений по безопасности и защите информации [Текст] / В.И. Ярочкин, Т.А. Шевцова. М., 2007.

47. *Ярочкин, В.И.* Система безопасности фирмы [Текст] / В.И. Ярочкин . М., 2008.

48. *Ярочкин, В.И.* Информационная безопасность [Текст] / В.И. Ярочкин. М., 2013.

Главный редактор — *Т. А. Смирнова*
Редакторы — *Н. П. Яшина, О. Л. Грозовская*
Художник — *Т. И. Такташов*
Верстка — *Е. В. Рудакова*
Корректор — *Н. Ф. Солодкова*
Ответственный за выпуск — *О. Л. Грозовская*

Кузнецов Игорь Николаевич

Бизнес-безопасность

Сертификат соответствия № РОСС RU.АВ51.НО5316

Подписано в печать 18.12.2020. Формат 60×90 1/16.
Бумага офсетная № 1. Печ. л. 25,75. Тираж 30 экз. Заказ №161580

Издательско-торговая корпорация «Дашков и К°»
129347, Москва, Ярославское шоссе, д. 142, к. 732
Тел.: 8 (495) 668-12-30, 8 (499) 182-01-58
E-mail: sales@dashkov.ru — отдел продаж;
office@dashkov.ru — офис; http://www.dashkov.ru

Отпечатано: Акционерное общество
«Т8 Издательские Технологии»
109316, Москва, Волгоградский проспект, дом 42, корпус 5
Тел.: 8 (499) 322-38-30