И. Н. Кузнецов

БИЗНЕС-БЕЗОПАСНОСТЬ

Бизнес-безопасность

«Дашков и К»
2018

УДК 65.012
ББК 65.290

Бизнес-безопасность / «Дашков и К», 2018

ISBN 978-5-394-02913-4

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.

УДК 65.012
ББК 65.290

ISBN 978-5-394-02913-4

Содержание

Игорь Кузнецов
Бизнес-безопасность

5-е издание, пересмотренное

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

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 интеллектуаль-

ных ресурсов, при котором гарантируются стабильность функционирования, 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 отечественный 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 подслушивающих 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 противо-

пожарную 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 вторые – 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 представителями 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 электронной 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 (СВ) 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.

Конец ознакомительного фрагмента.