БЕЗОПАСНОСТЬ МАЛЫХ И СРЕДНИХ ОБЪЕКТОВ ТОРГОВЛИ И УСЛУГ: КОМПЛЕКСНЫЙ ПОДХОД

Брединский Анатолий Геннадьевич
основатель и руководитель проекта «Безопасность для всех» (www.sec4all.net), ст. преподаватель кафедры «Защита, охрана и безопасность» ГУФКиС РМ

КОМПЛЕКСНЫЕ СИСТЕМЫ

С проблемой криминальных посягательств на учреждения торговли и сферы обслуживания сталкиваются практически все владельцы бизнеса.

Однако если крупные предприятия, расположенные преимущественно в больших городах, в той или иной мере озабочены проблемой собственной безопасности и решают ее в зависимости от своих возможностей, то для небольших магазинов, салонов, ломбардов, заправочных станций и других объектов, расположенных на периферии, эта проблема стоит наиболее остро. Характерно, что владельцы подобных учреждений часто весьма легкомысленно относятся к обеспечению безопасности своего бизнеса. Среди них бытует заблуждение, что малые объемы и удаленное расположение сами по себе являются надежной гарантией от посягательств правонарушителей. На самом же деле это не так.

Можно в очередной раз напомнить, что на каждую жертву обязательно найдется свой преступник и что многих как раз привлекают такие предприятия, так как в них нередко накапливаются серьезные денежные суммы или хранятся значительные материальные ценности. При этом их защита весьма условна или отсутствует вовсе. Кроме этого, подобные объекты часто становятся объектом посягательств со стороны социально опустившихся местных жителей – алкоголиков, наркоманов, лиц без определенного места жительства, начинающих малолетних преступников, которые при этом могут вести себя цинично и агрессивно.

Излишне напоминать, что в некоторых регионах уровень преступности в разы выше, чем в городах, а раскрываемость преступлений, к сожалению, оставляет желать лучшего.

Можно ли этому что-либо противопоставить и как защитить свой бизнес – об этом мы поговорим в рамках данной статьи.

С ЧЕГО НАЧИНАЕТСЯ ПРЕСТУПЛЕНИЕ?

Далеко не каждый владелец бизнеса задумывается, что значительная часть хищений имущества совершается не спонтанно. Ей предшествует этап подготовки, в ходе которого злоумышленники выбирают себе потенциальную жертву путем сбора необходимой информации об объеме и времени скопления денежной выручки, наличию и расположению материальных ценностей, графике работы того или иного объекта, системе его защиты и охраны, уязвимых местах и т.п. Иногда в качестве источника информации выступают работники предприятия, которые могут быть как соучастниками преступника, так и просто снабжать злоумышленника информацией, не задумываясь о возможных последствиях.

Даже молодые, только начинающие свою криминальную «карьеру» преступники практически никогда не выбирают для кражи (и тем более – разбоя) не знакомые им предприятия. Как и хищник, преступник предпочитает выбирать наиболее уязвимую и слабозащищенную жертву, нападение на которую позволит достигнуть положительного результата с наибольшей вероятностью.

Этот этап наиболее важен, так как обнаружение признаков подготовки преступления, а также противодействие им, позволит избежать возможных негативных последствий. Существуют определенные, наиболее типичные признаки того, что преступники проявляют интерес к конкретному объекту торговли и услуг. Отметим следующие:

- Периодическое появление вблизи объекта посторонних лиц, в том числе из местных жителей, без явной цели, но с проявлением видимого интереса к режиму работы объекта. В некоторых случаях оно может сопровождаться фотографированием или видеосъемкой, как маскируемой, так и явной. В отдельных случаях подобные действия могут производиться из припаркованных автомобилей.
- Внезапно участившиеся визиты лиц, не являющихся постоянными или давними клиентами, которые под различными предлогами задерживаются на объекте. В некоторых случаях они пытаются получить интересующую их информацию в ходе различных бесед с персоналом.

- Проявление чрезмерного интереса к режиму работы, системе безопасности, объемам и месту хранения денег и материальных ценностей со стороны обслуживающего персонала, особенно если они были недавно приняты на работу, либо со стороны лиц, осуществляющих временные работы (монтаж, уборка, ремонт, погрузочно-разгрузочные работы).
- Попытки проникнуть в служебные помещения, особенно в места хранения материальных ценностей со стороны посетителей или иных лиц, которые объясняются ошибками («Ошибся дверью», «Я в бухгалтерию», «Ищу туалет»).
- Неудачные попытки проникновения на охраняемый объект путем подбора ключей, попыток взлома дверей, окон или иными способами.
- Участившиеся перебои в работе технических средств охраны, которые могут быть результатом действия преступников.
- Увеличившееся число тревожных сигналов охранной сигнализации. Зачастую преступники намеренно провоцируют срабатывание сигнализации для выявления скорости реакции и тактики действий охраны.
- Проявление необоснованного повышенного интереса к работе предприятия со стороны работников, особенно из числа недавно принятых.
- Резкое изменение поведения работников (например, участившиеся задержки на работе, увеличившиеся личные траты, злоупотребление спиртными напитками и т.п.).

Естественно, этот перечень не является исчерпывающим и требует постоянного и серьезного внимания к тому, что происходит на предприятии. Именно своевременное выявление признаков подготовки преступления позволит успешно его избежать.

КАДРЫ РЕШАЮТ ВСЕ!

В связи с этим, одной из важных задач сотрудников охраны предприятия, а при их отсутствии – персонала, является постоянное наблюдение за окружающей обстановкой и выявление подозрительных случаев. Администрации объекта следует проводить периодические инструктажи с персоналом, напоминать им о необходимости быть бдительными, доводить до их сведения информацию о возможных подозрительных действиях. К сожалению, практика показывает, что к подобной системе большинство относится чисто формально.

Большое распространение получили попытки возложения собственником предприятия ответственности за любую утрату или порчу имущества, в том числе являющиеся результатом преступных действий, – на подчиненных. В случае совершения кражи или разбойного нападения от работников требуют возместить причиненный ущерб. Некоторые бизнесмены даже считают, что именно такие действия заставят персонал более серьезно относиться к защите имущества предприятия, так как фактически они будут предотвращать собственные материальные потери.

Однако подобное следует признать порочным. Во-первых, в большинстве случаев эти действия являются противозаконными, и в случае их выявления собственник может быть привлечен к ответственности. Во-вторых, это крайне негативно влияет на лояльность персонала. Работники, поставленные в подобные условия, могут совершать хищения посредством краж и мошеннических действий, дабы компенсировать потери, которые были на них возложены.

Кроме того, это провоцирует формирование атмосферы недоверия, конфликтов в коллективе, недобросовестного исполнения служебных обязанностей и, в том числе, постоянную смену кадров, в результате которой предприятие теряет подготовленные ценные ресурсы.

Как минимум наивным следует признать довольно распространенное убеждение собственника, который ожидает, что персонал проявит героизм и будет рисковать своей жизнью и здоровьем, пытаясь защитить имущество предприятия от преступных посягательств. И речь даже не о надуманных обязанностях, большинство работников, будучи не готово к критической ситуации, не зная, как себя вести, просто не способно к адекватной реакции.

Решение подобных вопросов может производиться только в виде системного подхода, в ходе которого формируется дружеский коллектив с четко разделенными служебными обязанностями и системой поощрений и наказаний. Персонал должен уяснить, что любое преступное посягательство – это угроза не только имуществу собственника, но и непосредственно их здоровью и, возможно, жизни. А любые материальные потери также негативно повлияют на них, так как не будет возможности выплачивать премии, повышенные оклады, а в некоторых случаях, даже зарплату.

Поэтому очень многое зависит от бдительности сотрудников. Для начала необходимо разработать должностные инструкции с алгоритмом действий в критической ситуации. Для создания подобных инструкций целесообразно привлечь специалистов, имеющих практические знания и опыт в данной сфере. После того, как соответствующие инструкции будут разработаны и утверждены приказом руководителя предприятия, сотрудники проходят инструктаж и знакомятся с ними под роспись. Крайне важно не превращать подобное в пустую формальность.

В результате такого инструктажа и изучения инструкций работники предприятия должны четко знать:

- признаки потенциальных угроз и подготовки преступных действий в отношении предприятия;
- какие действия им следует предпринимать, если они обнаружили подозрительное поведение;
- к кому, когда и как следует обратиться с этой информацией;
- какие средства охраны установлены на объекте и как с ними взаимодействовать;
- как себя правильно вести в различных критических ситуациях;
- какая ответственность и в каком объеме ложится на них в случае кражи, грабежа или разбоя в отношении предприятия;
- в чем заключается система поощрений и наказаний за несоблюдение подобных инструкций.

Разъясняя персоналу тактику, следует довести до них идею о том, что не существует универсальных рецептов и каждый конкретный случай требует своего решения. Так, в целом ряде случаев смелые и решительные действия персонала позволяли предотвратить разбойные, в том числе вооруженные, нападения на предприятие. Но в то же время есть примеры, когда попытки оказания сопротивления нападающему приводили к причинению тяжкого вреда здоровью или смерти работников. Практика показывает, что неготовность к подобным ситуациям, отсутствие знаний о том, как необходимо действовать, страх перед возможными последствиями, в том числе наказания со стороны руководителя, в критической ситуации может провоцировать у работника панику и неадекватные поступки, которые лишь ухудшают ситуацию.

После закрепления теоретического материала необходимо провести практическую отработку. Ее целесообразно реализовывать в виде ролевых ситуаций с различными сценариями (кража, разбой, хулиганство, мошенничество и т.п.), в ходе которых участники не рассказывают о том, как они будут действовать, а на деле демонстрируют алгоритм в заданных условиях. В ходе таких «учений» можно быстро выявлять ошибочные действия и сразу давать рекомендации о том, как следует поступить. Сценарии могут повторяться с введением дополнительных усложняющих условий или иметь различные варианты развития событий, в зависимости от действий персонала.

Идеально, когда подобные действия проводятся в максимально приближенной к реальности обстановке, но при этом формируется положительная «живая» соревновательная атмосфера. Работников, которые проявили себя с лучшей стороны, следует публично выделить и поощрить, в том числе, материально.

ЗАЩИТА – В КОМПЛЕКСЕ

Естественно, работа с персоналом является не единственным элементом защиты. Владельцу не следует забывать об оборудовании на объекте инженерных средств защиты, установке технических средств охраны, системы видеонаблюдения и контроле доступа, противокражных системах и постах физической охраны. Все эти элементы формируют единое целое, дополняя друг друга.

ИНЖЕНЕРНЫЕ СРЕДСТВА ЗАЩИТЫ

Инженерные средства защиты представляют собой элементы конструкции или интерьера, целью которых является затруднение преступного посягательства на материальные ценности. К подобным средствам относятся строительные элементы (укрепленные конструкции, в том числе стены, полы и потолки), защитные двери и окна, решетки, роллеты, турникеты, шлагбаумы, сейфы, защитные шкафы и т.п.

К сожалению, многие объекты торговли не уделяют особого внимания этим средствам защиты. Даже в тех случаях, когда существуют рекомендуемые или даже обязательные требования к укрепленности объекта, они соблюдаются далеко не всегда. Зачастую торговые точки и учреждения сферы услуг размещаются в изначально не предназначенных для этого помещениях, при этом отсутствует время да и желание собственника что-либо менять.

Есть примеры, когда после переезда в помещение новых владельцев, предыдущие, зная уязвимые места, могли легко проникнуть на объект. В отдельных случаях для этого использовались ключи от замков, которые никто не посчитал нужным сменить. Именно поэтому перед открытием объекта производятся необходимые действия по оборудованию его необходимыми средствами инженерной защиты. Входные двери, особенно ведущие в торговые залы, складские и кассовые помещения устанавливаются с учетом максимальной взломостойкости. Если это возможно, их целесообразно установить в виде шлюза, одна за другой, таким образом, чтобы при вскрытии одной злоумышленник не имел свободного доступа и вынужден был заниматься взломом второй в условиях ограниченного пространства.

Окна оборудуются защитными роллетами или ставнями, которые препятствуют проникновению преступников и служат для защиты от повреждений, в том числе в результате действий природы (град, ураган). Весьма распространенная практика установки на окна решеток далеко не всегда эффективна, так как решетки устанавливаются с внешней стороны окна, что позволяет преступникам беспрепятственно производить с ними манипуляции (например, выдернуть их, зацепив тросом, прикрепленным к автомобилю). Кроме этого, в случае пожара, аварии или стихийного бедствия, решетки блокируют окна, не позволяя покинуть помещение. Более эффективным является установка внутренних раздвижных решеток или иных защитных элементов, взаимодействие с которыми невозможно без вскрытия окна.

Особое внимание следует уделить защите помещений, где хранятся денежные средства и материальные ценности. Располагать подобные помещения следует внутри объекта, желательно там, где нет внешних стен, выходящих на улицу или смежных с соседними помещениями, не принадлежащими собственнику. Материальные ценности, с которыми не осуществляется постоянные операции, а также не находящиеся без постоянного контроля, в обязательном порядке помещаются в защищенные шкафы или сейфы. Эта же процедура проделывается при покидании магазина персоналом, даже если оно краткосрочно (ночное время, выходные и праздничные дни, обед и т.п.).

В последние годы участились кражи, совершаемые группой лиц, нередко подростков. Вскрыв двери или разбив витрину, преступники быстро похищают товары, находящиеся в открытом доступе, и скрываются до приезда полиции или группы быстрого реагирования. За счет участия нескольких (иногда до 10) лиц, такие действия могут причинить значительный ущерб. В связи с этим, рекомендуется не оставлять ценные предметы вблизи к внешним окнам и дверям, укреплять внешние витрины защитными элементами (например, специальной защитной пленкой), крепить товары к стойкам и витринам или выставлять вместо них муляжи.

ОХРАННАЯ СИГНАЛИЗАЦИЯ

Оборудование объектов торговли и сферы услуг охраной сигнализацией является обязательной мерой. В ряде стран помещения, не оснащенные подобными системами, не подлежат страхованию, так как считается, что собственник не предпринял действия для сохранения своего имущества.

При оборудовании помещения охранной сигнализацией не следует экономить, так как наличие уязвимых мест и слепых зон в охране значительно снижает защищенность объекта. Целесообразно использование комбинированных извещателей охранной сигнализации, которые препятствуют их нейтрализации опытными преступниками. Установленная система охранной сигнализации подлежит постоянному контролю и проверке ее работоспособности. При необходимости осуществляется ее модернизация современными средствами. Особо внимательным к системе охранной сигнализации следует быть при проведении строительных и ремонтных работ на объекте. Нередко в ходе таких работ нарушается функциональность охранной сигнализации, появляются новые помещения, которые не оборудованы охранными средствами. Иногда собственники самостоятельно деактивируют сигнализацию на время проведения работ, чем могут воспользоваться преступники. Также не стоит забывать, что участившиеся сигналы тревоги или перебои в работе охранной сигнализации могут быть вызваны действиями преступников, которые таким образом добиваются снижения внимания или даже отключения охранной сигнализации.

СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ

Одними из самых распространенных технических средств безопасности, устанавливаемых на объектах малого и среднего бизнеса, являются камеры видеонаблюдения. И хотя эксперты утверждают, что системы видеонаблюдения предотвращают не более 10% криминальных посягательств, именно их собственники наиболее охотно устанавливают в своих торговых и сервисных залах.

Безусловно, польза от подобных систем есть. Во-первых, наличие видеонаблюдения на объекте, в тех случаях, когда осуществляется его мониторинг, позволяет выявить подозрительное поведение на этапе подготовки преступления. Во-вторых, в случае совершения нападения, будут получены ценные кадры происходящего, которые позволят точно понять, как именно действовали преступники. В ряде случаев именно с помощью записей систем видеонаблюдения удается получить изображения преступников, что даст возможность их идентифицировать и привлечь к ответственности. Даже если злоумышленники используют различные маскирующие внешность средства (маски, капюшоны и т.п.), видеозапись позволит эксперту получить ценную информацию о примерном росте, телосложении, ориентировочном возрасте преступников. А в некоторых случаях – их особые приметы или информацию об особенностях поведения (хромота, характерные жесты, действия, свидетельствующие о наличии преступного опыта и т.п.).

Однако следует упомянуть, что крайне часто владельцы бизнеса совершают типичные ошибки, не обладая достаточной компетенцией, но при этом активно желая сэкономить свои средства. Среди наиболее распространенных ошибок:

- выбор бюджетных камер от малоизвестных производителей;
- приобретение или использование давно устаревшего оборудования, не соответствующего современным требованиям;
- использование некачественного программного обеспечения;
- установка видеонаблюдения таким образом, чтобы оно, в основном, следило

за сотрудниками, в результате, при криминальных посягательствах такие камеры становятся малоэффективными.

Также следует упомянуть о весьма распространенной проблеме с организацией хранения видеоархива. Нередко он ведется бессистемно, не осуществляется должного контроля наличия записей и их хранения. Встречаются ситуации, когда запись вовсе не ведется в результате сбоев в работе регистратора или заполнения носителей информации. А владелец бизнеса узнает об этом лишь после совершения преступления, когда выясняется, что никаких записей нет.

Соответственно, чтобы видеонаблюдение стало эффективным элементом системы безопасности, требуется серьезный подход к выбору таких систем, их установке и обслуживанию. Необходимо внедрить современные программные средства видеоаналитики, которые значительно упрощают работу оператору. Не менее важно грамотно подобрать тип камер и правильно установить их на объекте, без «слепых зон». И, конечно, необходимо организовать хранение и архивацию видеоданных.

В некоторых случаях, на этапе подготовки преступления злоумышленники могут попытаться вывести камеры из строя (например, распылить на объектив лак или краску), изменить угол обзора камеры или предпринять какие-то другие действия. Данные факты должны быть своевременно выявлены операторами, и предприняты необходимые меры защиты.

Отдельного внимания заслуживает вопрос о соблюдении при видеонаблюдении нормативных положений о защите персональных данных, которым в последнее время уделяется все большее внимание.

КОНТРОЛЬ ДОСТУПА

К сожалению, система контроля и управления доступом (СКУД) не пользуется большой популярностью на средних и малых объектах торговли и услуг, особенно расположенных на периферии. Владельцы бизнеса предпочитают на этом экономить. На самом деле, это большая ошибка. Помимо вспомогательных функций по контролю за персоналом (время прихода и ухода с работы, контроль за опозданиями и перемещениями в течение рабочего дня) такие системы позволяют предотвратить незаконное проникновение в служебные помещения, в том числе, с целью кражи.

Практика показывает, что нередки случаи, когда преступники в течение рабочего дня свободно проникают в служебные помещения, пользуясь отсутствием должного контроля со стороны работников, где похищают денежные средства и материальные ценности, в том числе принадлежащие сотрудникам.

Иногда такие хищения совершаются и самими работниками, которые, обнаружив в открытых помещениях ценности, предпочитают их присвоить, оставаясь безнаказанными. Поэтому наряду с иными техническими средствами, такими как охранная сигнализация и видеонаблюдение, целесообразна установка систем контроля доступа, особенно в тех помещениях, где хранятся значительные материальные ценности или конфиденциальная информация предприятия.

ПРОТИВОКРАЖНЫЕ СИСТЕМЫ

К сожалению, количество хищений из торговых залов постоянно растет и принимает масштабы эпидемии. Среди молодых людей даже стал популярным шоплифтинг (от англ. shop – магазин и lift – поднимать, тягать), т.е. кражи, совершаемые зачастую не из корыстных, а скорее из хулиганских побуждений, «на спор», чтобы хвастаться этим перед знакомыми.

Подобные действия способны наносить огромный ущерб розничной торговле, при этом, ни наличие видеонаблюдения, ни охранники в торговом зале или персонал не способны полноценно противостоять. Одним из решений подобных ситуаций выступают противокражные системы, которые позволяют обнаруживать попытки выноса товаров, оснащенных специальными радиочастотными метками без оплаты на кассе. Естественно, что подобные системы не являются абсолютной гарантией от кражи, однако способны значительно снизить число хищений и, потенциально, заставить злоумышленников отказаться от своих планов.

ХИМИЧЕСКИЕ ЛОВУШКИ, МАРКИРОВОЧНЫЕ СРЕДСТВА

К сожалению, химические ловушки и маркировочные средства не являются распространенными элементами защиты. Большинство владельцев бизнеса даже не имеют о них элементарных представлений.

Вместе с тем, химическая ловушка – это оснащенные или обработанные специальными химическими веществами (красящими, люминесцирующими или запаховыми) приспособления или устройства, которые могут быть закамуфлированы под различные предметы (денежная пачка, образец товара, материальная ценность). Их также могут устанавливать в местах хранения ценностей (касса, сейф, склад), чтобы при попытке кражи ловушка срабатывала. В результате взаимодействия с такими средствами происходит окрашивание или маркировка похищенного либо непосредственно преступника специальными веществами, которые позволяют их дальнейшее обнаружение. Например, специальные вещества из химической ловушки способны окрасить злоумышленника ярким, хорошо заметным цветом, крайне устойчивым к попыткам его удалить. При наличии у правоохранительных органов образцов краски или маркирующего вещества дальнейшее обнаружение преступника или похищенного значительно упрощается. Однако не следует в этом вопросе прибегать к кустарным, самодельным устройствам, так как одним из требований к химическим ловушкам является их абсолютная безопасность для человека. Также следует помнить, что подобные средства не способны работать по принципу «свой/чужой», т.е. могут сработать и в отношении работника предприятия, клиента или иного лица, которое не было предупреждено или забыло об их наличии.

АКТИВНЫЕ СРЕДСТВА ЗАЩИТЫ

Большинство из вышеперечисленных технических средств охраны по своей сути являются пассивными. Т.е. они способны лишь обнаруживать тревожное событие или фиксировать произошедшее, непосредственные же действия должны предприниматься человеком. Однако опыт показывает, что в случае разбойных нападений или тщательно подготовленных краж их может быть не достаточно. В связи с этим получили распространение системы активной защиты, одной из которых являются генераторы тумана. Это специальные устройства, которые по ручному или автоматическому сигналу тревоги способны быстро заполнять замкнутые помещения непрозрачным туманом. В результате злоумышленник теряет ориентацию в пространстве и не способен завершить свои преступные намерения. Практика применения таких систем показывает, что чаще всего преступники предпочитают ретироваться в первые же секунды после срабатывания такой системы. При этом вещества, формирующие непрозрачный туман, не пачкают и не повреждают товары, они безвредны для человека. Подобные системы могут быть эффективны при разбойных нападениях, когда оказание сопротивления вооруженным преступникам может вызвать агрессию с их стороны и нанесение телесных повреждений сотрудникам охраны или персоналу.

ВЫВОДЫ

Подводя итоги, мы приходим к выводу, что легкомысленное отношение к защите своего бизнеса и желание сэкономить на безопасности приводит к печальным последствиям. Материальный ущерб даже от одной кражи, грабежа или разбоя способен превысить затраты на обеспечение безопасности. Поэтому к данному вопросу важно отнестись серьезно, применяя комбинированный комплексный подход и доверяя решение специалистам. Ведь стабильность и спокойствие, особенно, если они не ложные, – крайне важны для успеха бизнеса.