Ограбление по-русски

Е.П. Тюрин

Банки всегда служили притягательными объектами для различных преступных элементов. Концентрация значительных денежных и материальных ценностей в одном месте и кажущаяся возможность быстрого завладения ими вынуждает преступников постоянно думать о совершенствовании своих методов как организационно, так и технически. А руководство банка, в свою очередь, – заботиться о соответствующих адекватных мерах по обеспечению безопасности.

Система комплексной безопасности банка должна обеспечивать достаточно высокую надежность защиты банков от всех возможных внутренних и внешних видов угроз и опасных ситуаций. Комплексная безопасность объединяет в себе три основные составляющие: физическая безопасность, инженерно-техническая безопасность и информационная безопасность.

В свою очередь, каждая из этих составляющих включает в себя несколько подсистем. **Физическая безопасность** охватывает такие аспекты, как личностная безопасность (решает вопросы личной охраны служащих банка и членов их семей), кадровый подбор сотрудников банка и проверка их на благонадежность, а также любые вопросы, связанные с безопасностью личности. В структуру **инженерно-технической безопасности** могут входить: техническая укрепленность (инженерная защита) банка, охранно-пожарная сигнализация с системами пожаротушения и дымоудаления, системы контроля и управления доступом, системы охранного телевидения, системы сбора и обработки информации и другие системы, связанные с предотвращением угрозы имущественных потерь. **Информационная безопасность** подразумевает защиту от утечки информации посредством физических полей и сред, сопутствующих работе, а также программную безопасность (утечка информации посредством внедрения в компьютерные сети банков).

Каждая из перечисленных выше составляющих, входящих систему безопасности, имеет свои особенности и сложности. В настоящей статье будут рассмотрены только некоторые вопросы инженерно-технической безопасности как наиболее важные и непосредственно влияющие на сохранность денежных, материальных и иных ценностей банков.

От эффективности организации инженерно-технической безопасности зависит сохранение всех ценностей банка при угрозе их похищения или уничтожения. В свою очередь, уровень безопасности зависит от времени реагирования системы безопасности на предполагаемую угрозу и от времени ликвидации этой угрозы: чем меньше время реагирования, тем выше уровень безопасности.

Весь процесс похищения условно можно разделить на четыре основных этапа.

Первый этап – период подготовки к краже. Как правило, преступное посягательство на банк или его структурные подразделения происходит не спонтанно. Изучается объект нападения, выбираются оптимальные методы и средства проникновения на него. В этот период, хотя и имеются объективные и субъективные предпосылки возможного посягательства на банк, никакого непосредственного ущерба ему пока не наносится. Можно предположить следующее: чем надежнее оборудован банк различными системами безопасности, тем дольше процесс их изучения и больше вероятность того, что соответствующие профилактические мероприятия и меры по предупреждению возможного возникновения угрозы смогут остановить нападение.

Второй этап – преодоление злоумышленником конструкционных и защитных инженерных сооружений, таких, как стены, двери, окна, решетки и т.п. Злоумышленник с помощью специального инструмента старается проникнуть в помещения банка, где хранятся ценности (хранилища, сейфовые комнаты, сейфы, металлические шкафы и т.д.), которые заблокированы охранной сигнализацией. Естественно, чем прочнее указанные конструкции и защитные инженерные сооружения, тем больше времени приходится злоумышленнику тратить на их преодоление и тем больше шансов у служб безопасности или подразделений милиции пресечь вторжение.

В настоящее время выпущено достаточно много ГОСТов и нормативных документов, определяющих требования к строительным и защитным конструкциям, их элементам. Неукоснительное выполнение этих норм – залог надежной защиты любого банка. При проектировании системы безопасности банка следует руководствоваться следующими основными документами:

1. ГОСТ Р 51053-97. Замки сейфовые. Требования и методы испытаний на устойчивость к криминальному открыванию и взлому.

2. ГОСТ Р 51136-98. Стекла защитные многослойные. Общие технические условия.

3. ГОСТ Р 50862-96. Сейфы и хранилища ценностей. Требования и методы испытаний на устойчивость к взлому и огнестойкость.

4. ГОСТ Р 50941-96. Кабина защитная. Общие технические требования и методы испытаний.

5. ГОСТ Р 51110-97. Средства защитные банковские. Общие технические требования.

6. ГОСТ Р 51111-97. Средства защитные банковские. Правила приемки и методы испытаний.

7. ГОСТ Р 51112-97. Средства защитные банковские. Требования по пулестойкости и методы испытаний.

8. ГОСТ Р 51113-97. Средства защитные банковские. Требования по устойчивости к взлому и методы испытаний.

9. ГОСТ Р 51222-98. Средства защитные банковские. Жалюзи. Общие технические условия.

10. ГОСТ Р 51224-98. Средства защитные банковские. Двери и люки. Общие технические условия.

11. Инструкция № 241Р от 10.06.97. Требования по технической укрепленности и оборудованию сигнализацией, системами контроля доступа и видеоконтроля учреждений Сбербанка России (с дополнениями №1-4).

12. Инструкция № 227 от 15.01.96. Требования к оборудованию учреждений Центрального Банка Российской Федерации техническими средствами охраны.

13. ВНП 001 - 01 Банк России. Ведомственные нормы проектирования. Здания территориальных главных управлений, национальных банков и расчетно-кассовых центров Центрального банка Российской Федерации.

14. Указание Центрального банка Российской Федерации от 23.04.01 №960-У. О внесении изменений в Положение Банка Росси от 25 марта 1997 года №56 «О порядке ведения кассовых операций в кредитных организациях на территории Российской Федерации».

Третий этап – непосредственное проникновение злоумышленника в помещение или сейф с ценностями. Каких-либо сложностей, за исключением охранных ловушек, или «кукол», в этот период времени у злоумышленника уже нет. И чем больше времени имеется у него, тем больший ущерб банку он может нанести.

Четвертый этап – фактическая ликвидация угрозы или опасной ситуации. Основные функции по ликвидации в этот период принимают на себя силы служб безопасности или группы задержания подразделений милиции.

Очевидно, что, чем раньше можно обнаружить несанкционированное воздействие или проникновение злоумышленника в банк, тем эффективнее можно пресечь попытку и избежать материального ущерба. Поэтому от правильного размещения технических средств охраны в банке, от того, как установлены защитные инженерно-технические конструкции, как учтены вероятные угрозы и пути возможного проникновения злоумышленника в охраняемую зону банка, зависит оперативное пресечение действий злоумышленника и сохранение материальных ценностей.

Рассмотрим реальную ситуацию: *оконный проем одного банка заблокирован решетками и извещателями разбития стекла с наружной стороны окна, а в другом банке решетка и извещатель установлены с внутренней стороны окна. Чтобы попасть в помещение первого банка, злоумышленнику необходимо сначала перепилить решетку, затем разбить стекло. Во втором случае, соответственно, все происходит наоборот. Понятно, что второй вариант для охраны более предпочтителен, так как извещатель, контролирующий разбитие стекла, обнаружит нарушителя сразу же и выдаст тревожное извещение на пульт охраны. Времени, которое необходимо злоумышленнику на взлом решетки, установленной за разбитым стеклом (около четырех минут), будет достаточно для прибытия группы задержания подразделения милиции или службы безопасности банка и принятия ими соответствующих мер по пресечению преступных действий. В первом же случае у злоумышленника больше шансов на успех, так как процесс разрушения решетки не будет обнаружен извещателем. Сигнал тревоги поступит на пульт охраны только лишь при разбитии оконного стекла. Запаса времени у группы задержания в этом случае уже не будет.*

Однако нельзя не сказать о том, что достаточно часто кражи происходят не только из-за неправильного размещения технических средств охраны, но и по причине неумения правильно оценить возможные вероятные угрозы.

Можно привести еще один случай, *произошедший в одном филиале банка, оборудованном в соответствии со всеми требованиями руководящих документов. Двери, стены, окна и небольшой сейф имели соответствующий класс устойчивости к взлому и три рубежа охранной сигнализации (периметр банка с запасной и входной металлическими дверями, объем помещений, сейф, в котором хранились ценности), выведенной на пульт охраны.*

Группа злоумышленников с помощью фомки, кувалды и других подручных «инструментов» взломала запасную дверь, причем, по словам жителей соседних домов, эта операция длилась достаточно продолжительное время, но сигнал тревоги на пульт охраны не поступал. Запасная металлическая дверь была заблокирована охранной сигнализацией на пролом проводом, а на открывание – магнитоконтактным извещателем. Злоумышленники так ювелирно «работали» инструментами, что взломали замки и открыли дверь, не оборвав охранный провод. Только после открытия двери сработал охранный извещатель и сигнал тревоги поступил в пункт охраны. Группа задержания немедленно выехала. Но преступники подготовились к ограблению. Они хорошо знали расположение помещений, места хранения ценностей, и расчет у них был только на внезапность и быстроту. После первого тревожного извещения, на пульт охраны поступает второй сигнал

(от объемных извещателей), и сразу же за ним – третий (от сейфа, в котором размещались денежные купюры). Прибыв примерно через три минуты, группа задержания обнаружила следующую картину: дверь взломана, а сейфа в помещении нет. Грабители не стали взламывать сейф, а просто унесли его вместе с ценностями.

Анализ случившегося показывает, что не все было учтено и продумано при проектировании системы безопасности банка. Ограбление не произошло бы или злоумышленники были бы задержаны, если бы в банке сделали следующее:

1. За входной дверью установили бы дополнительную, решетчатую дверь, закрываемую на замок (требование РД.78.147-93). Взломав входную дверь, злоумышленники «попотели» бы и над решетчатой дверью, но запаса времени у них уже не было, так как «сработала» бы охранная сигнализация при открывании входной двери.

2. Входную дверь защитили бы от взлома извещателем раннего обнаружения (таким, например, как, «Шорох»). В этом случае можно было бы не только избежать ограбления, но и сохранить дверь от повреждений. Ведь указанный тип извещателя реагирует на различные механические воздействия на охраняемый предмет, в том числе на ударные.

3. Сейф с денежной наличностью, который похитили, прикрепили бы к полу или стене. Это требование указано в ГОСТ Р 50862-96. (Сейфы и хранилища ценностей): «Сейфы и металлические шкафы массой менее 1000 кг должны крепиться с помощью анкерного крепления к полу или стене либо встраиваться в стену».

В данной статье хочется также заметить, что во многих случаях хищения и ограбления банков, как у нас в России, так и за рубежом, происходят по вине технических средств охраны. Хотя если разобраться, то в 90 % случаев виновата не техника, а неправильная установка или несоответствие технических характеристик приборов требованиям охраняемого объекта и поставленным задачам. Предполагаемое в проектной документации размещение мебели или других крупногабаритных предметов в охраняемых зонах часто не соответствует тому, что на самом деле в них находится после сдачи банка в эксплуатацию. Естественно, зоны обнаружения извещателей меняются, что ведет к проблемам с обнаружением злоумышленников, плохой помехоустойчивости.

Необходимо учитывать, что радиоволновые извещатели, в отличие от оптико-электронных, допускают маскировку материалами, пропускающими радиоволны (ткани, древесно-стружечные плиты, стекло). Их можно устанавливать внутри офисной мебели, за стеклянными створками и драпировочными тканями. Однако при такой установке дальность действия радиоволновых извещателей будет меньше, чем в свободном пространстве. На практике этот факт зачастую не учитывается. Кроме того, если извещатель устанавливается в узком коридоре,

дальность его действия увеличивается в 1,5–2 раза. А если в торце коридора, расположенного на первом этаже, есть оконный проем, возможна выдача извещения о тревоге при движении людей или механизмов за пределами охраняемого помещения (данный недостаток устраняется уменьшением дальности действия извещателей).

Отметим также, что охранные извещатели должны обладать разнообразными принципами обнаружения попыток проникновения. При этом существует мнение, что достаточно поставить некоторое количество так называемых «объемников», и вопрос можно считать закрытым. На самом деле, все намного сложнее, и не каждая проектно-монтажная организация готова работать в банках.

Есть и положительный момент в разработке системы безопасности банков: широкая номенклатура отечественных извещателей (как по типам, так и по техническим характеристикам), которые не уступают, а во многом и превосходят зарубежные аналоги по своим техническим характеристикам. В качестве примера хотелось бы привести извещатель **«Сова 2»**. В одном корпусе этого прибора размещено сразу два извещателя: объемный пассивный инфракрасный (реагирует на любые перемещения злоумышленника в охраняемых помещениях) и поверхностный звуковой (регистрирует все попытки воздействия на оконные стекла). Кроме того, инфракрасный канал извещателя защищен акустическим каналом от попыток возможного саботажа его нормального функционирования. За счет наличия трехпозиционного держателя встроенного микрофона этот извещатель может быть установлен практически в любом удобном месте, максимально обеспечив защиту объема помещений от проникновения. Уникальность его состоит еще и в том, что он регистрирует попытки проникнуть не только через обычное стекло, но и через все типы стеклянных защитных композиций по классу А1–А3, которые используются. За рубежом извещателей с такими возможностями еще не выпускают.

Как показал зарубежный и отечественный опыт, при выполнении всех требований к технической укрепленности и охранной сигнализации вероятность несанкционированного проникновения в банки становиться ничтожно малой. Но попытки нападения на кредитные учреждения в рабочее время предпринимаются часто. При этом преступники берут в заложники сотрудников или клиентов. В данном случае для вызова дополнительных сил (группы задержания подразделения милиции) используется тревожная сигнализация. С ее назначением и возможностями знаком даже начинающий работник банковского бизнеса.

К сожалению, не всегда имеется возможность без риска для жизни нажать кнопку или педаль на рабочих местах кассиров или в местах хранения ценностей. Большую помощь здесь может оказать **радиосистема тревожной сигнализации «Радиокнопка».** Небольшие по размерам, очень похожие на сотовые телефоны радиопередатчики, размещенные в карманах или, что еще лучше – на поясе, помимо самой кнопки, имеют датчик падения. Его нормальное положение – вертикальное, антенной вниз. Достаточно на время (более 15 секунд) наклонить этот передатчик на угол 45–70°, и сразу будет передано тре-

вожное извещение. Если сотрудник охраны выполняет приказ «лечь на пол», то автоматически срабатывает датчик падения. В случае производственной необходимости этот датчик простым нажатием кнопки может быть отключен на 5 минут. Такие радиопередатчики имеет смысл носить как старшим кассирам, так и сотрудникам кладовых ценностей. Из опыта последних лет следует также, что наиболее часто нападение на инкассаторов происходит на участке «инкассаторский бронеавтомобиль – вход в кредитную организацию». Здесь тоже могла бы пригодиться такая система.

Уже не первый год в кладовых ценностей и на рабочих местах кассиров размещены ловушки типа «Мини-кредит» и «Кукла-Л», или датчики последней купюры типа «Клипса». Их использование, впрочем, не всегда удобно. Идущие к «Куклам» и «Клипсам» провода, как правило, мешают привычной работе кассиров. Этот недостаток учтен, и в настоящее время разработан и запускается в производство тревожный извещатель **«Радиокукла»**. Это модернизированный радиопередатчик радиосистемы тревожной сигнализации с датчиком падения, помещенный в 100-листовую упаковку банковских купюр. Работает эта «Радиокукла» аналогично «Радиокнопке» и совместима с уже имеющимися на объектах приемниками. Если преступник спутает эту купюру с другими, и положит в сумку, то будет подан сигнал тревоги. Хранить ее можно в кладовой на стеллажах или в сейфах, а также на рабочих местах кассиров.

В заключение хотелось бы отметить, что всплеск разбойных нападений на кредитные учреждения, имевший место в середине 90-х годов, сведен практически к минимуму. Постепенно техническая укрепленность и средства охраны в большинстве отечественных банков начинают соответствовать международным требованиям, что в итоге не может не сказаться на их имиджевой привлекательности.

Из вышесказанного следует, что только при условии качественно проведенной подготовительной работы и постоянного повседневного внимания к вопросам обеспечения безопасности всех составляющих банка можно рассчитывать на своевременность и оперативность в отражении предполагаемой угрозы или чрезвычайной ситуации.