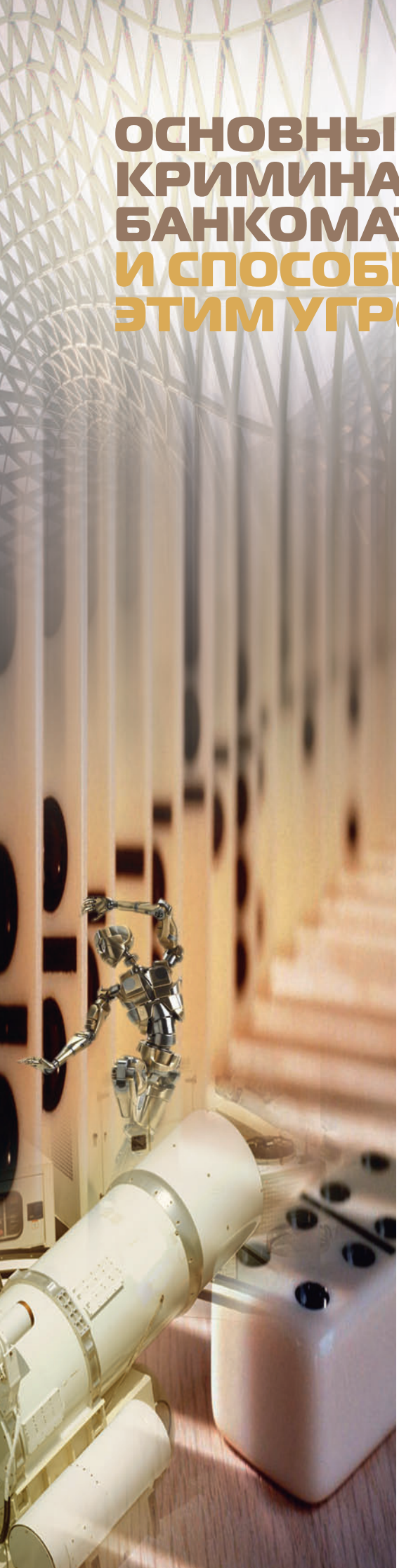


ОСНОВНЫЕ ВИДЫ КРИМИНАЛЬНЫХ УГРОЗ БАНКОМАТАМ И СПОСОБЫ ПРОТИВОДЕЙСТВИЯ ЭТИМ УГРОЗАМ

А. Климов
заместитель начальника отдела ФКУ НИЦ «Охрана» МВД России, полковник полиции,
Н. Рябцев
научный сотрудник ФКУ НИЦ «Охрана» МВД России, лейтенант полиции

В продолжение темы противокриминальной защиты банкоматов, начатой в предыдущей статье «Современная классификация банковских устройств самообслуживания и мест их размещения», опубликованной в № 2 (2015), в данной публикации мы рассмотрим основные категории нарушителей и виды совершаемых ими преступлений на объектах дистанционного банковского обслуживания, а также известные на сегодня способы противодействия таким преступлениям.
Анализ статистики преступлений, связанных с противоправными посягательствами на банкоматы (платежные терминалы), позволяет из всего многообразия нарушителей выделить несколько основных категорий.

1. ОДНА ИЗ НАИБОЛЕЕ РАСПРОСТРАНЕННЫХ КАТЕГОРИЙ НАРУШИТЕЛЕЙ – ВЗЛОМЩИКИ

Целью таких нарушителей является кража наличных денег из нижнего кабинета (сейфа) банкомата, нередко сопряженная с незаконным проникновением в помещение, где установлен банкомат. Для достижения этой цели они используют три основных способа:

- взлом сейфа банкомата на месте его размещения;
- криминальное открывание замка сейфа банкомата;
- несанкционированное перемещение (кража) банкомата и вскрытие его в удаленном месте.

Для взлома сейфа банкомата «медвежатники» чаще всего используют обычный слесарный инструмент (ручной или электрический), который свободно можно приобрести в строительном магазине (кувалду, лом, ножовку, дисковую пилу типа «болгарка», газовый резак и т.п.). Однако в последнее время участились и случаи разрушения оболочки сейфа банкомата посредством взрыва. Для этого злоумышленники либо закачивают в нижний кабинет банкомата взрывоопасный газ, либо устанавливают кумулятивный заряд снаружи сейфа.

Криминальное открывание запирающего устройства сейфа банкомата осуществляется чаще всего с помощью специализированного инструмента (отмычек), позволяющего открыть замок без использования ключа или его разрушения, а в некоторых случаях – путем использования штатных ключей или кодов (если имел место сговор преступников с работниками кредитной или обслуживающей организации).

Для несанкционированного перемещения банкомата злоумышленники используют подручные, автотранспортные или специальные средства. С помощью данных средств преступники извлекают банкомат из помещения и увозят в удаленное скрытое место, где и осуществляют непосредственный взлом сейфа и изъятие наличных денежных средств.

Если же банкомат или платежный терминал размещен в закрытом помещении (иными словами к нему нет свободного доступа в любое время суток), нарушителям приходится сначала проникнуть в помещение, «обойти» средства охранной сигнализации и видеонаблюдения (при их наличии), и только после этого добираться до наличности, взламывая сейф банкомата. Как показывает статистика такого рода преступлений, нарушителей не останавливает даже наличие физической охраны на объекте, особенно в виде пожилого сторожа или вахтерши.

Указанными видами преступлений занимаются как кустари-одиночки с простейшими подручными инструментами, так и организованные преступные группы, оснащенные по последнему слову техники.

Для противодействия такого рода преступлениям, прежде всего, необходимо соблюдение требований по инженерно-технической укрепленности как самого банкомата, так и помещения, в котором он ус-

тановлен. Данные вопросы достаточно подробно отражены в Рекомендациях Р 78.36.035-2013 МВД России [1].

Кроме того, на рынке систем безопасности имеется целый арсенал технических средств охранной сигнализации, с помощью которых можно построить достаточно надежную защиту банкоматов. Начнем с самого, пожалуй, важного этапа построения такой защиты – выбора средств обнаружения несанкционированного проникновения нарушителей в зону размещения банкомата и совершения криминальных воздействий на него.

Для блокировки «на открывание» дверных и оконных конструкций помещения, в котором установлен банкомат, а также открываемых или перемещаемых конструкций самого банкомата, обеспечивающих доступ к нижнему кабинету (сейфу) или верхнему кабинету (процессорному блоку), обычно используют магнитоконтактные извещатели, которые должны соответствовать требованиям ГОСТ Р 54832-2011 [2], с учетом видов, размеров и материалов охраняемых конструкций.

При выборе конкретных типов магнитоконтактных извещателей, устанавливаемых внутри банкомата, в частности, для блокировки «на открывание» основной двери нижнего кабинета необходимо учитывать ограничения по размерам свободного пространства, связанные с высокой плотностью расположения внутренних механизмов (кассет с наличными деньгами), периодически перемещаемых и извлекаемых при инкассации, а также при обслуживании и ремонте.

Для блокировки «на открывание» пластиковой декоративной двери нижнего кабинета банкомата (при ее наличии) рекомендуется использовать магнитоконтактные извещатели, обладающие функцией защиты от саботажа внешним магнитным полем, чтобы нарушитель, воспользовавшись мощным магнитом, не мог вывести магнитоконтактный извещатель из строя, а если кто и попытается это сделать, то извещатель должен подать сигнал тревоги.

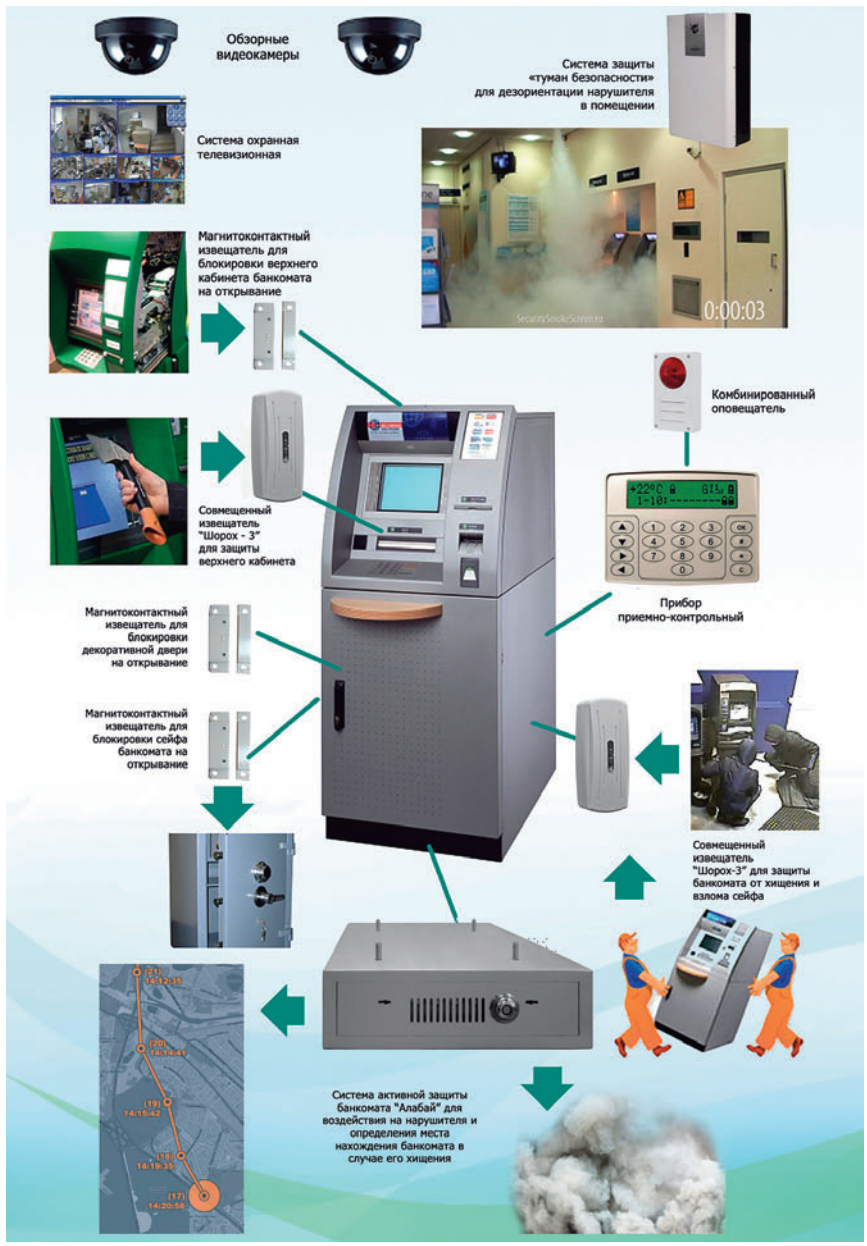
Для обнаружения разрушения обычных и защитных стекол, стеклопакетов, а также стекол со специальными свойствами, применяемых для остекления помещений, как правило, используют акустические (звуковые) извещатели, которые должны соответствовать требованиям ГОСТ Р 51186-1998 [3], а также обладать функциями активной защиты от маскирования и автоматического контроля работоспособности.

Для обнаружения попытки умышленного разрушения, повреждения или взлома ограждающих строительных и защитных конструкций помещения, в котором установлен банкомат, особенно, если данные конструкции не обладают высокой степенью устойчивости к взлому, рекомендуется использовать специальные вибрационные извещатели, которые должны соответствовать требованиям ГОСТ Р 53702-2009 [4], обнаруживать все типы разрушающих воздействий по ГОСТ Р 50862-2012 [5] и выбираться в соответствии с видами, размерами и материалами охраняемых конструкций.

Для обнаружения проникновения нарушителя через дверной или оконный проем помещения, в котором установлен банкомат, рекомендуется использовать оптико-электронные (инфракрасные) извещатели не ниже 3 класса по ГОСТ Р 50777-2014 [6], имеющие поверхностную зону обнаружения типа «занавес».

Для обнаружения перемещения нарушителя в помещении, в котором установлен банкомат, целесообразно использовать не менее двух извещателей с объемной зоной обнаружения, имеющих также функцию защиты от маскирования, принцип действия которых (по крайней мере, одного из них) должен отличаться от принципа действия извещателя, используемого для обнаружения проникновения через оконный

и дверной проемы данного помещения. Например, оптико-электронный извещатель не ниже 3 класса по ГОСТ Р 50777-2014 [6] совместно с радиоволновым извещателем по ГОСТ Р 50659-2012 [7] или ультразвуко-



вым извещателем по ГОСТ Р 50658-1994 [8]. В некоторых случаях используют комбинированные извещатели – оптико-электронный с радиоволновым по ГОСТ Р 52650-2006 [9] или оптико-электронный с ультразвуковым ГОСТ Р 55150-2012 [10].

Для обнаружения взлома непосредственно нижнего кабинета (сейфа) банкомата или вскрытия корпуса платежного терминала, встроенного в капитальную строительную конструкцию, могут быть использованы вышеуказанные вибрационные извещатели.

А вот банкоматы, которые обособленно установлены внутри или снаружи помещений, должны быть защищены не только от взлома, но и от несанкционированного перемещения (кражи целиком). Для такой комплексной защиты рекомендуется использовать совмещенные извещатели, в состав которых входят соответствующие каналы обнаружения на основе датчиков вибрации и перемещения (наклона), специально предназначенные для использования в банкоматах и обладающие чувствительностью ко всем возможным видам криминальных воздействий на банкомат и помехозащищенностью (в том числе к работе механизмов выдачи денег и печати чеков). Извещатели также должны иметь соответствующие функции защиты от вскрытия и нарушения функционального механического контакта с контролируемой конструкцией банкомата.

Для защиты от криминального открывания замка сейфа банкомата необходимо применение замков высокого класса устойчивости к криминальному открыванию и взлому по ГОСТ Р 52582-2006 [11], в том числе оборудованные устройствами раннего реагирования, например, в виде датчика перемещения засова.

Отдельной проблемой является защита банкомата от вскрытия его нижнего кабинета (сейфа) с помощью взрывных устройств. Для противодействия, скажем так, легкому и быстрому вскрытию банкомата взрывной волной его сейф должен быть, по меньшей мере, 3 класса устойчивости к взлому по ГОСТ Р 50862-2012 [5] и иметь специальную маркировку «EX». Это означает, что после взрыва злоумышленникам еще придется повозиться какое-то время, чтобы получить доступ к кассетам с деньгами. За это время у службы охраны есть шанс успеть прибыть на объект и задержать нарушителей на месте преступления.

2. Следующая категория правонарушителей, связанная с банкоматами, – «грабители»

Это наиболее опасный вид преступников, действующих в сфере дистанционного банковского обслуживания. Под угрозу вооруженного ограбления могут попасть как обычные граждане (при снятии наличных денег из банкомата), так и инкассаторы (при загрузке, выгрузке или транспортировке наличных денежных средств). В этой категории встречаются как отчаянные «одиночки», так и организованные преступные группы, имеющие специальные знания, подготовку, автотранспорт, средства подавления радиосвязи, огнестрельное оружие.

Для противодействия этой категории преступников необходимо оснащение банкоматов системами «интеллектуального» видеонаблюдения, а также средствами тревожной сигнализации. Кроме того, на обсуждение может быть вынесен вопрос о негласном формировании сигнала тревоги путем набора специальной комбинации цифр на панели ввода ПИН-кода.

3. Третья, весьма распространенная категория нарушителей, – это так называемые киберпреступники, или хакеры

Их цели и методы «работы» могут быть различными. В одних случаях – это может быть кража наличных денег из нижнего кабинета банкомата, в других – получение незаконного доступа к конфиденциальной информации банковских карт клиентов.

В первом случае, в отличие от вышеописанных взломщиков, хакерам нужен непосредственный доступ не в нижний кабинет банкомата, где расположены кассеты с наличными деньгами, а в верхний кабинет банкомата, где расположен компьютерный блок с операционной системой. Путем вскрытия верхнего кабинета и несанкционированного подключения к компьютеру банкомата они устанавливают вредоносные программы или подменяют программное обеспечение банкомата. После чего банкомат становится «послушным» и либо выдает деньги из своего нижнего кабинета по команде нарушителя, либо осуществляет безналичные переводы денежных средств с чужих счетов, к которым был получен доступ.

В связи с этим, для обеспечения безопасности банкомата от таких угроз, необходимо, во-первых, заблокировать (защитить от несанкционированного открывания) верхний кабинет, например, с помощью магнитоконтактного извещателя. Во-вторых, обеспечить программную защиту операционной системы и программного обеспечения банкомата от хакерских атак.

Достаточно вспомнить, какого шума в конце 2014 года наделал вирус Backdoor.MSIL.Tyupkin, обнаруженный «Лабораторией Касперского». Этот вирус заражал банкоматы по всему миру и позволял киберпреступникам опустошать кассеты с деньгами. При этом на Россию пришелся самый большой процент «ограблений» банкоматов с его помощью. Как сообщили эксперты «Лаборатории Касперского», ограбления совершались без использования кодов карт физлиц путем прямых манипуляций с банкоматами. Специалисты проанализировали видеоматериалы с камер видеонаблюдения, которые были установлены в местах размещения зараженных банкоматов, и выявили, что злоумышленники получали деньги из банкоматов, предварительно установив вредоносный код с загрузочного диска. Этот вирус оказался актуальным для банкоматов, работающих на 32-разрядной платформе Microsoft Windows.

После проведения расследования по новому вирусу «Лабораторией Касперского» были разработаны практические рекомендации [12] для кредитно-финансовых организаций, компаний, занимающихся обслуживанием банковских устройств самообслуживания, и разработчиков программного обеспечения (ПО) для банкоматов. В соответствии с этими рекомендациями во избежание рисков заражения банкоматов вредоносными программами необходимо:

- усилить физическую защиту банкоматов (важно, чтобы банкомат надежно стоял на месте – был прикреплен к стене или полу помещения либо помещен в специальный бокс);
- установить охранную сигнализацию (по данным «Лаборатории Касперского» Backdoor.MSIL.Tyupkin заражал только банкоматы без сигнализации);
- заменить все замки и мастер-ключи от производителя, запирающие верхние отсеки (кабинеты) банкоматов;
- сменить установленные по умолчанию пароли BIOS (разработчикам ПО следует, в целом, уделять больше внимания безопасности устройств: уникальные пароли BIOS должны быть сложными, состоящими не только из цифр, но и букв, и спецсимволов);
- установить и регулярно обновлять антивирусную защиту банкоматов;
- регулярно выполнять полную проверку файловой системы каждого банкомата;
- регулярно проверять банкоматы на наличие сторонних устройств (скиммеров);
- использовать только проверенные Whitelisting-продукты на банкоматах, чтобы снизить вероятность определения антивирусами чистого программного обеспечения как вредоносного и наоборот.

4. Четвертой, широко распространенной категорией нарушителей являются мошенники

Эта криминальная категория наиболее «разношерстная» и изобретательная. Цели таких правонарушителей и методы их деяний могут быть различными, порой непредсказуемыми. Отметим лишь наиболее известные:

- кража конфиденциальной информации банковских карт клиентов (скимминг);
- кража банковской карты путем ее механической блокировки в картридере банкомата («ливанская петля»);

- кража наличных денег клиента путем захвата и удержания банкнот в презентере банкомата;
- ложная отмена банковской или платежной операции;
- установка подложных банкоматов («банкоматов-клонов»);
- создание «сайтов-клонов» кредитных организаций;
- рассылка на сотовые телефоны держателей банковских карт сообщений от имени банка о блокировке банковской карты.

Проблемы борьбы с мошенничеством в сфере дистанционного банковского обслуживания требуют отдельного обстоятельного разговора.

Также в отдельной статье стоит рассмотреть вопросы организации видеонаблюдения и охранного телевидения в зоне размещения банкоматов, платежных терминалов и других средств дистанционного банковского обслуживания, а также особенности применения систем активной защиты, устанавливаемых как в самих банкоматах, так и в клиентских зонах. В настоящее время данные направления в области безопасности объектов дистанционного банковского обслуживания активно развиваются и позволяют существенно повысить эффективность применяемых мер защиты.

ЛИТЕРАТУРА

1. *Р 78.36.035-2013 МВД России «Рекомендации по организации комплексной централизованной охраны банковских устройств самообслуживания».*
2. *ГОСТ Р 54832-2011 Извещатели охранные точечные магнитоконтактные. Общие технические требования и методы испытаний.*
3. *ГОСТ Р 51186-1998 Извещатели охранные звуковые пассивные для блокировки остекленных конструкций в закрытых помещениях. Общие технические требования и методы испытаний.*
4. *ГОСТ Р 53702-2009 Извещатели охранные поверхностные вибрационные для блокировки строительных конструкций закрытых помещений и сейфов. Общие технические требования и методы испытаний.*
5. *ГОСТ Р 50862-2012 Сейфы, сейфовые комнаты и хранилища ценностей. Требования и методы испытаний на устойчивость к взлому и огнестойкость.*
6. *ГОСТ Р 50777-2014 Извещатели пассивные оптико-электронные инфракрасные для закрытых помещений и открытых площадок. Общие технические требования и методы испытаний.*
7. *ГОСТ Р 50659-2012 Извещатели радиоволновые доплеровские для закрытых помещений и открытых площадок. Общие технические требования и методы испытаний.*
8. *ГОСТ Р 50658-1994 Системы тревожной сигнализации. Часть 2. Требования к системам охранной сигнализации. Раздел 4. Ультразвуковые доплеровские извещатели для закрытых помещений.*
9. *ГОСТ Р 52650-2006 Извещатели охранные комбинированные радиоволновые с пассивными инфракрасными для закрытых помещений. Общие технические требования и методы испытаний.*
10. *ГОСТ Р 55150-2012 Извещатели охранные комбинированные ультразвуковые с пассивными инфракрасными для закрытых помещений. Общие технические требования и методы испытаний.*
11. *ГОСТ Р 52582-2006 Замки для защитных конструкций. Требования и методы испытаний на устойчивость к криминальному открыванию и взлому.*
12. *Голованов С. Банкоматный вирус Tyupkin: будут ли новые атаки? // Банкноты стран мира. М., 2015. № 4. С. 26-27.*