# ОЦЕНКА РИСКА НАРУШЕНИЯ КИБЕРБЕЗОПАСНОСТИ В КОММЕРЧЕСКОМ БАНКЕ (НА ПРИМЕРЕ АТАК НА БАНКОМАТЫ “BRUTE FORCE” И “BLACK BOX”)

***Ревенков П.В.[1], Бердюгин А.А.[2], Макеев П.В.[3]***

***Аннотация.*** *В течение XX–XXI в. произошло развитие технологий, в результате которого была создана глобальная финансовая система, позволяющая быстро совершать денежные транзакции в противоположных точках Земли. Прогресс цифровой трансформации общества и, в частности, финансово-экономических систем приводит к усложнению проблем информационной безопасности конкурирующих субъектов. Делая основной упор на научных исследованиях, можно достичь успеха в этих вопросах.*

***Цель исследования:*** *повышение уровня защищённости банковского обслуживания физических и юридических лиц в соответствии с рекомендациями стандартов по информационной безопасности посредством анализа риска нарушения информационной безопасности в банковских технологиях (на примере атак “Brute force” и “Black box”).*

***Методы исследования:*** *эмпирические методы научного познания (наблюдение, измерение, эксперимент), теоретические методы (анализ, синтез, индукция, дедукция, абстрагирование, формализация), графическая интерпретация информации, методы теории вероятностей и компьютерное программирование.*

***Результат исследования:*** *рассмотрены стандарты для осуществления эффективного управления информационной безопасностью на предприятии. Количественно показано преимущество методов социальной инженерии над методом перебора (“Brute force”) PIN-кодов. Проанализированы временны́е характеристики её совершения и защитные меры от атак типа “Black box”. Предложен метод повышения эффективности реагирования и защиты банкоматов от атак типа “Black box”.*

***Ключевые слова:*** *стандарты, PIN-код, вероятность подбора, ATM, диспенсер, киберпреступник, продолжительность кибератаки.*

**DOI:**10.21681/2311-3456-2021-3-20-30

## Введение

Модернизация финансовых услуг усложняет финансовые технологии и добавляет к деятельности банков и их рисковому портфелю больше разнообразия и комплементарности. За прошедшие десятилетия условия деятельности коммерческих банков всех стран мира претерпели существенные изменения. Факторы научно-технического прогресса привели как к появлению новых финансовых инструментов и возможностей банков [1], так и к необходимости управления совершенно новыми видами рисков в соответствии с новыми стандартами [2], о которых пойдёт речь в статье.

Серия международных стандартов ISO/IEC 27000 включает стандарты по информационной безопасности, опубликованные совместно Международной Организацией по Стандартизации (ISO) и Международной Электротехнической Комиссии (IEC). Набор состоит из лучших практик и рекомендаций в области информационной безопасности для создания, развития и поддержания системы менеджмента информационной безопасности (СМИБ). Комплексное применение этих технических документов изображено на рис. 1. Каждый из них направлен на исследование определённых задач по управлению информационной безопасностью.

Кроме этого, комплекс документов по стандартизации Центрального банка Российской Федерации содержит единый подход к обеспечению информационной безопасности организаций банковской системы (ИББС) и рекомендации по стандартизации (РС) с учётом требований российского законодательства. Фундаментальный стандарт в рассматриваемой сфере – СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения», цели и задачи которого приведены на https://cbr.ru/information_security/Gubzi_docs/ [3].

1 Ревенков Павел Владимирович, доктор экономических наук, доцент, профессор Департамента информационной безопасности, Финансовый университет при Правительстве Российской Федерации, Москва, Россия. E-mail: pavel.revenkov@mail.ru, orcid.org/0000-0002-0354-0665

2 Бердюгин Александр Александрович, младший научный сотрудник Департамента информационной безопасности, Финансовый университет при Правительстве Российской Федерации, Москва, Россия. E-mail: brdgn@bk.ru, orcid.org/0000-0003-2301-1776

3 Макеев Павел Владимирович, магистрант Факультета информационных технологий и анализа больших данных, Финансовый университет при Правительстве Российской Федерации, Москва, Россия. E-mail: paulmakeev@gmail.com, orcid.org/0000-0003-0031-5419

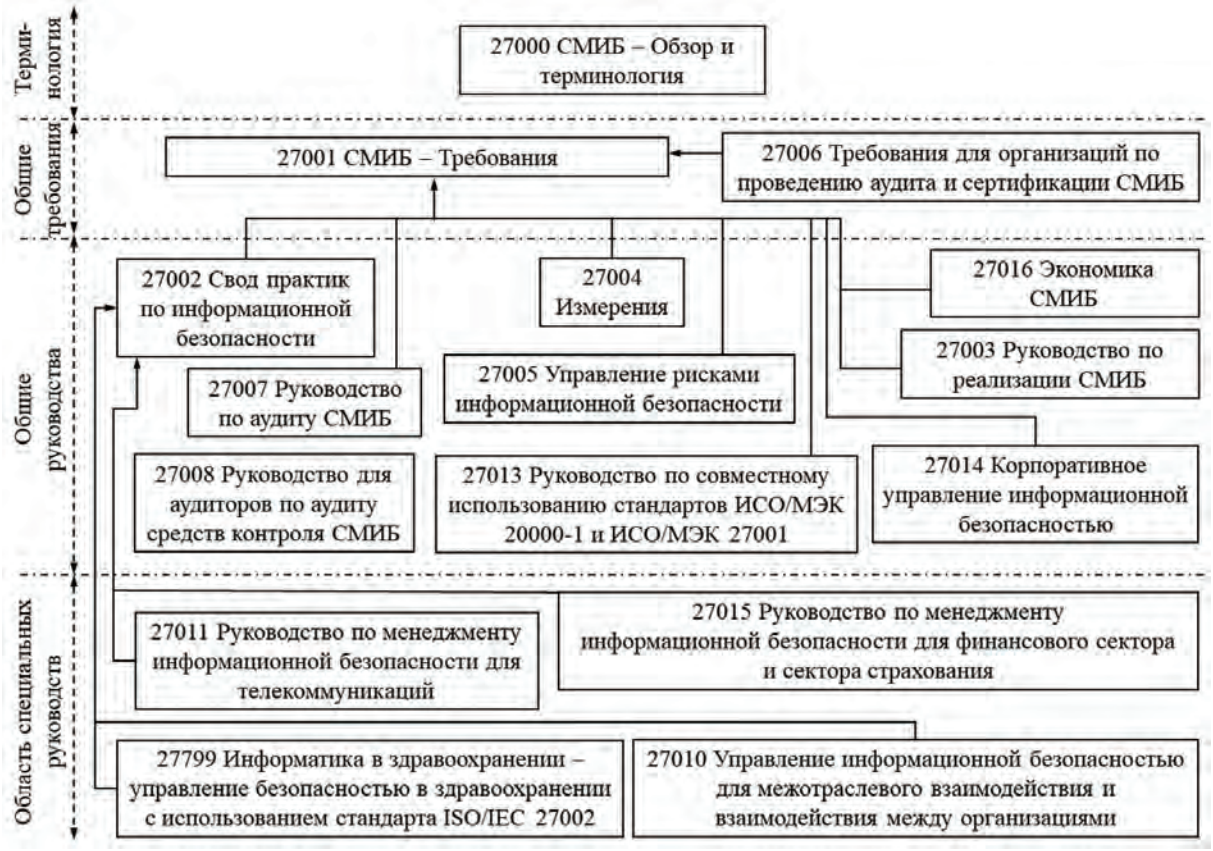


*Рис. 1. Структура нормативов и стандартов серии ISO/IEC 270xx*[4]


*Рис. 2. Система обеспечения информационной безопасности организации банковской системы России*

4 Воронин А.С. Национальная платежная система. Бизнес-энциклопедия. М.: КНОРУС: ЦИПСиР, 2013. 424 с.

Ознакомиться с перечисленными стандартами можно в соответствующем разделе сайта Банка России[5]. Взаимосвязь СМИБ, системы обеспечения информационной безопасности (СОИБ) и системы информационной безопасности (СИБ) организаций банковской системы России отображена на рис. 2.

Согласно СТО БР ИББС-1.0-2014, разница между СМИБ, СИБ и СОИБ состоит в следующем:

СИБ – это совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение.

СМИБ – часть менеджмента организации банковской системы России, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и совершенствования системы обеспечения информационной безопасности.

СОИБ – совокупность СИБ и СМИБ организации банковской системы России.

Киберпространство – важная составная часть современного общества. Если одна страна запустит масштабную атаку на электростанции или коммерческие банки другой страны, то могут быть предприняты ответные военные меры не только в виртуальном, но и в реальном мире. Кибератака, нарушающая нормальное функционирование, приводящая к панике, массовым волнениям или человеческим жертвам, может вызвать громкий силовой ответ [4].

Решение большинства проблем и задач кибербезопасности должно иметь научную базу. При выполнении коллективной научно-исследовательской и/или опытно-конструкторской работы стандарты и нормативно-правовые акты, описанные в техническом задании (ТЗ, техзадание) к выполняемой работе, для исполнителей носят не рекомендательный, а обязательный ко внимательному прочтению характер. В противном случае может сложиться ситуация, описанная в басне И.А. Крылова «Квартет».

### Атаки на банкоматы: “Brute force” и социальная инженерия

Статистика по данным Банка России показывает, что основной причиной реализации кибератак в банковской сфере является дезинформирование (97% в 2018 г. и 92% в 2017 г.). Для юридических лиц этот показатель составил 39%[6].

PIN-код банковской карты содержит 4 цифры от 0 до 9. Игнорируя реальную ситуацию, когда после трёх неправильных наборов PIN-кода банкомат блокирует или «проглатывает» карточку, а также учитывая, что перебор всех возможных комбинаций PIN-кода (“Brute force”) по технической части не сложнее приёмов социальной инженерии, определим время, необходимое для перебора.

Количество возможных комбинаций PIN-кода $N = 10^4 - 10 = 9990$ (совместное появление десяти цифр на 4 позициях за исключением номеров с четырьмя одинаковыми цифрами).

1. Вероятность подбора на первой попытке $P_1 = 1/N$;

2. Произведение вероятности $1/(N-1)$ (на 1 попытку меньше) и условной вероятности после первой попытки $1-\frac{1}{N} = \frac{N-1}{N}$ определяет вероятность подбора на второй попытке $P_2 = \frac{1}{N-1}\cdot\frac{N-1}{N} = \frac{1}{N}$.

3. Произведение вероятности $1/(N-2)$ (на 2 попытки меньше), условной вероятности после второй попытки $1-\frac{1}{N-1} = \frac{N-2}{N-1}$ и условной вероятности после первой попытки (известна) $1-\frac{1}{N} = \frac{N-1}{N}$ определяет вероятность подбора на третьей попытке $P_3 = \frac{1}{N-2}\cdot\frac{N-2}{N-1}\cdot\frac{N-1}{N} = \frac{1}{N}$;

4. Произведение вероятности $1/(N-3)$ (три попытки позади), условной вероятности после третьей попытки $1-\frac{1}{N-2} = \frac{N-3}{N-2}$, условной вероятности после второй попытки (известна) $1-\frac{1}{N-1} = \frac{N-2}{N-1}$ и условной вероятности после первой попытки (известна) $1-\frac{1}{N} = \frac{N-1}{N}$ определяет вероятность подбора на четвёртой попытке $P_3 = \frac{1}{N-2}\cdot\frac{N-2}{N-1}\cdot\frac{N-1}{N} = \frac{1}{N}$;

На любой попытке вероятность угадывания киберпреступником PIN-кода $P_N = \frac{1}{N}$ [5]. Математическое ожидание количества попыток – произведение вероятности и суммы первых *N* членов арифметической прогрессии

$$M_N = \frac{1}{N}\cdot 1 + \frac{1}{N}\cdot 2 + \ldots + \frac{1}{N}\cdot N = \\ = \frac{1}{N}\cdot(1+2+\ldots+N) = \frac{1}{N}\cdot\frac{(N+1)\cdot N}{2} = \frac{N+1}{2} \quad (1)$$

Пусть продолжительность одной попытки подбора $5\text{ сек.} = \frac{5}{60\cdot 60}\text{ час.} = \frac{1}{720}\text{ час.}$ Тогда математическое ожидание продолжительности подбора PIN-кода $\frac{9991}{2\cdot 720} \approx 6{,}9\text{ час.}$ Этого времени достаточно, чтобы сотрудники банка заподозрили неладное и вызвали полицию.

Фрагмент программного кода в среде Borland Delphi, иллюстрирующего оценку продолжительности

5 Информационная безопасность. Правовые акты. URL: https://cbr.ru/information_security/acts/?la.Search=&la.TagId=&la.VidId=26&la.Date.Time=Any&la.Date.DateFrom=&la.Date.DateTo= (дата обращения 22.02.2021).

6 Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019–2021 годов. М.: Центральный банк Российской Федерации, 2019, 26 с. URL: https://www.cbr.ru/Content/Document/File/83253/onrib_2021.pdf (дата обращения 20.02.2021).

“Brute force”, приведён ниже.

```
procedure TForm1.Button1Click(Sender: TObject);
var
  k, t: extended; { комбинации пароля, время одной проверки }
  l, n: integer;  { длина пароля, кол-во возможных символов }
begin
  if (Edit1.Text = '') or (Edit2.Text = '')
    or (Edit3.Text = '')
  then ShowMessage('Пожалуйста, заполните все поля!') else
  begin
    l := StrToInt(Edit1.Text);
    n := StrToInt(Edit2.Text);
    t := StrToInt(Edit3.Text);

    k := exp(l*ln(n)); { кол-во комбинаций n^l = e^(l*ln(n)) }
    t := t/3600;       { перевод секунд в часы }
    Label4.Caption := FloatToStr((k+1)*t/2) + ' час.';
  end;
end;
```

Приёмы социальной инженерии ограничиваются минутами, что делает очевидным преимущество их умелого применения для киберпреступника [6]. На сегодняшний день при эксплуатации новой SIM-карты перечень контактов пополняется только справочными номерами (Service Dialing Numbers – SDN) оператора мобильной связи (часть из них сразу удаляется самим абонентом). Предложение авторов состоит в том, чтобы SDN содержали номера некоторых кредитных организаций и Банка России. Это позволит:

- заинтересовать пользователя (поняв, зачем нужны номера кредитных организаций, он сам добавит нужные);
- определять входящий номер телефона (банк или жулик);
- побудить клиента самостоятельно перезвонить в банк, если ему позвонили «из службы безопасности Вашего банка».

Таким образом, организуется сотрудничество: сотовые операторы прописывают в SDN SIM-карты телефоны известных банков, банки рекламируют этих операторов на своих пластиковых картах, клиенты повышают свою грамотность и безопасность.

### Кибератаки типа “Black box” на банкоматы

Обеспечение безопасности банковских информационных систем является сложным процессом, выполняемым по ряду различных методик и требующим соблюдения множества стандартов, таких как СТО БР ИББС, ГОСТ Р ИСО/МЭК 15408 и PCI DSS [7]. Но в случае с банкоматами (Automated teller machine, ATM) зачастую реализуют безопасность через неизвестность (путём сокрытия информации о внутренних подсистемах банкомата, интерфейсах и протоколах взаимодействия компонентов). Это затрудняет атаки, но не гарантирует безопасность.

Значительной угрозой для банковской сферы являются аппаратно-программные комплексы, предназначенные для хищения денежных средств из банкоматов, которые называются “Black box” – аппаратура со специальным программным обеспечением (ПО), подключающаяся к диспенсеру (механизму выдачи денег) вместо рабочего компьютера экспертов коммерческого банка. Далее управление банкоматом переходит в руки киберпреступников, и передача данных осуществляется с помощью бесконтактных технологий (например, со смартфона) [8].

Так, согласно статистике по кибератакам типа “Black box” за 2012–2018 год [9], наблюдается стремительный рост количества случаев во всех странах из выборки (рис. 3).

Статистика, опубликованная в Отчёте о преступлениях в европейских платёжных терминалах (табл. 1) [10], свидетельствует о повышении количества инцидентов логических атак на ATM на 269% по сравнению с 2019 г. Стоит уточнить, что все зафиксированные за 2020 логические кибератаки являются атаками типа “Black box”. По результатам отчёта 22-й встречи EAST EGAF, атаки типа “Black box” занимают второе место по количеству случаев, уступая лишь «скиммингу» [11]. Также стоит упомянуть сообщения о появлениях новых способов проведения кибератаки данного типа в 2020 г. [10], что свидетельствует о востребованности методов данной атаки и интересе к ней киберпреступников.

По информации директора по безопасности BI.ZONE [12], число кибератак с применением технических средств увеличилось на 4% от общего числа атак в 2019 году. Он связывает это с благоприятными условиями в виде мер против COVID-19: почти все киберпреступники использовали медицинские маски в качестве маскировки.

DOI:10.21681/2311-3456-2021-3-20-30


*Рис. 3. Количество зафиксированных случаев атак типа "Black box" в различных странах*

*Таблица 1*

*Статистика кибератак на платёжные терминалы и банкоматы (European payment terminal crime statistics – summary)*[7]

| **Terminal Related Fraud Attacks** | H1 2016 | H1 2017 | H1 2018 | H1 2019 | H1 2020 | % +/– 19/20 |
|---|---|---|---|---|---|---|
| Total reported Incidents | 10,820 | 11,934 | 6,760 | 10,723 | 3,631 | –66% |
| Total reported losses | €174m | €124m | €107m | €124m | €109m | –12% |
| | | | | | | |
| **ATM Related Physical Attacks** | H1 2016 | H1 2017 | H1 2018 | H1 2019 | H1 2020 | % +/– 19/20 |
| Total reported Incidents | 1,604 | 1,696 | 2,046 | 2,376 | 1,829 | –23% |
| Total reported losses | €27m | €12.2m | €15.1m | €11.4m | €12.6m | +11% |
| | | | | | | |
| **ATM Malware & Logical Attacks** | H1 2016 | H1 2017 | H1 2018 | H1 2019 | H1 2020 | % +/– 19/20 |
| Total reported Incidents | 28 | 114 | 61 | 35 | 129 | +269% |
| Total reported losses | €0.41m | €1.51m | €0.25m | €0.00m | €1.00m | N/A |

Source: European Association for Secure Transactions (EAST)

Учитывая перечисленные факты, можно утверждать, что атаки типа "Black box" являются актуальным и опасным вектором нападения в текущих реалиях несмотря на применяемые банками защитные меры. Рассмотрим их основные характеристики и приведём актуальные методы защиты.

**Основные характеристики атак типа "Black box"**

Согласно материалам отчёта Positive Technologies [11], "Black box" является кибератакой логического типа, которая позволяет похитить деньги из сейфа АТМ. Она выполняется путём подключения специального устройства к шине диспенсера, с целью отправки на

7 European Association for Secure Transactions. Black Box attacks increase across Europe. URL: https://www.association-secure-transactions.eu/black-box-attacks-increase-across-europe/ (дата обращения 10.03.2021).


*Рис. 4. Классификация атак на банкоматы*


*Рис. 5. Схема выполнения кибератаки на банкоматы типа "Black box"*

него неавторизованных команд для вывода наличных средств. На схеме (рис. 4) указано расположение атак данного типа в общей классификации банковских атак на основе материалов статьи [13].

Для выполнения атаки типа "Black box" необходимо устройство с контроллерами интерфейсов для подключения к порту диспенсера и программное обеспечение для управления им. Типовыми интерфейсами являются RS232, RS485 или USB. В качестве устройства управления обычно применяются одноплатные компьютеры или ноутбуки по причине их мобильности. Для подключения "Black box"-устройства необходимо отключить диспенсер от блока управления банкоматом, но в случае использования протокола RS485 возможно подключение параллельно. Также зафиксированы случаи использования смартфонов, управляемых извне, в качестве "Black box"-устройств [8]. Рассмотрим схему выполнения атаки типа "Black box" (рис. 5). На ней указано расположение основных функциональных блоков, взаимосвязь между ними и место внедрения киберпреступника при совершении кибератаки.

Перечислим ключевые характеристики атак типа "Black box":

1) злоумышленнику необходимо получить доступ к интерфейсу диспенсера или центральной шине устройств АТМ;
2) взаимодействие с диспенсером АТМ происходит с отдельного устройства, поэтому атака не оставляет следов о совершаемых операциях в журналах безопасности;

3) для подготовки “Black box”-устройства от киберпреступника требуются знания внутреннего устройства АТМ и его ПО;
4) успех атаки не зависит от операционной системы (ОС), процессингового центра и ПО для управления АТМ;
5) использование официальных утилит от разработчиков банковского ПО для взаимодействия с диспенсером. Обычно утилиты имеют защиту от злонамеренного использования, но киберпреступники обходят её изменением кода программы [14].

**Продолжительность совершения кибератаки “Black box”**

Получив представление о методе совершения атаки и требуемых для этого ресурсах, проанализируем временные характеристики её совершения.

По материалам аналитической статьи [13], средняя продолжительность выполнения атаки данного типа составляет 10 минут. Для получения более точных данных необходимо рассмотреть каждую из стадий совершения атаки:
1) вскрытие сервисной зоны банкомата – $T_v$. В зависимости от способа продолжительность колеблется от 3 секунд до 2 минут;
1.1) использование физического ключа (подлинного или копии) для открытия шкафа сервисной зоны ($T_{v1}$) – несколько секунд;
1.2) вскрытие замка шкафа сервисной зоны ($T_{v2}$) – от 30 до 60 секунд;
1.3) вырезание отверстия в лицевой панели банкомата ($T_{v3}$) – от 60 до 150 секунд.
2) подключение “Black box”-устройства к интерфейсу или шине данных ($T_p$). В зависимости от навыков киберпреступника, процесс занимает от 20 до 60 секунд.
3) изъятие денежных средств через диспенсер ($T_i$). В зависимости от модели сейф банкомата вмещает до 8000 банкнот разного номинала, которые находятся в четырёх специальных кассетах.

Банкомат содержит от 3 до 14 миллионов рублей. Такой разброс вызван рядом факторов, таких как: тип банкомата, место его установки, скорость расхода банкнот и сумма страхования. Средняя сумма средств, обычно находящаяся в банкомате универсального типа при полной загрузке, составляет порядка 7–8 млн руб. За один раз диспенсер извлекает из сейфа максимум 40 купюр, а задержка между операциями составляет 20 секунд [15]. Таким образом, полное извлечение купюр из сейфа займёт 4000 секунд (1 час 7 минут), что составляет от 200 000 руб. до 4000 руб. за 20 секунд. Согласно информации о совершённых атаках, каждая процедура изъятия денежной наличности занимала от 1 до 3 часов [16].

Информация о временны́х рамках совершения операций была получена путём анализа видеоматериалов[8] в свободном доступе и сведений от экспертов в области атак на АТМ.

Решающим фактором, ограничивающим продолжительность кибератаки ($T_a$), являются действия определённых средств защиты, в том числе срабатывания сигнализации и приезд наряда полиции. Нормативы прибытия правоохранительных органов не регламентируются законодательно, но обычно минимальное время прибытия наряда полиции или сотрудников частного охранного предприятия ($T_n$) составляет 4–7 минут.

$$T_a < T_n \tag{2}$$

Процесс совершения кибератаки состоит из трёх этапов, и продолжительность её выполнения может быть представлена как:

$$T_a = T_v + T_p + T_i \tag{3}$$

Первые две стадии являются подготовительными этапами, а последняя стадия – процессом извлечения денежных средств.

$$T_a = T_{подг.} + T_{извл.} \tag{4}$$

Рассмотрим минимально и максимально возможную продолжительность совершения подготовительной стадии кибератаки:

$$T_{подг.\ min} = T_{v1\,min} + T_{p\,min} = 3\,\text{сек.} + 20\,\text{сек.} = 23\,\text{сек.} \tag{5}$$

$$T_{подг.\ max} = T_{v3\,max} + T_{p\,max} = 150\,\text{сек.} + 60\,\text{сек.} = 210\,\text{сек.} \tag{6}$$

Процесс извлечения денежных средств будет выполняться вплоть до прибытия сил охраны правопорядка:

$$T_{извл.} = T_n - T_p \tag{7}$$

Тогда максимальная и минимальная продолжительность извлечения равна:

$$T_{извл.\ min} = T_{n\,max} + T_{подг.\ min} = 420\,\text{сек.} - 23\,\text{сек.} = 217\,\text{сек.} \tag{8}$$

$$T_{извл.\ max} = T_{n\,min} + T_{подг.\ max} = 240\,\text{сек.} - 210\,\text{сек.} = 30\,\text{сек.} \tag{9}$$

Раз в 20 секунд АТМ выдаёт 40 купюр, следовательно, если получать купюры максимального номинала (5000 руб.), то можно извлечь 200 000 руб. раз в 20 секунд.

Таким образом, максимальная и минимальная сумма денежных средств, которую киберпреступник успевает извлечь до приезда правоохранительных органов равна:

$$S_{max} = \frac{T_{извл.\ min}}{20\,\text{сек.}} \cdot 5000\,\text{руб.} = \frac{217\text{сек.}}{20\,\text{сек.}} \cdot 5000\,\text{руб.} = 2\,000\,000\,\text{руб.} \tag{10}$$

$$S_{min} = \frac{T_{извл.\ max}}{20\,\text{сек.}} \cdot 5000\,\text{руб.} = \frac{30\,\text{сек.}}{20\,\text{сек.}} \cdot 5000\,\text{руб.} = 200\,000\,\text{руб.} \tag{11}$$

8 По материалам доклада «Hack Your ATM with Friend's Raspberry.Py» Black Hat 2015. URL: https://www.youtube.com/watch?v=q5tQWe6YsLM, 15:57 (дата обращения 15.01.2021).

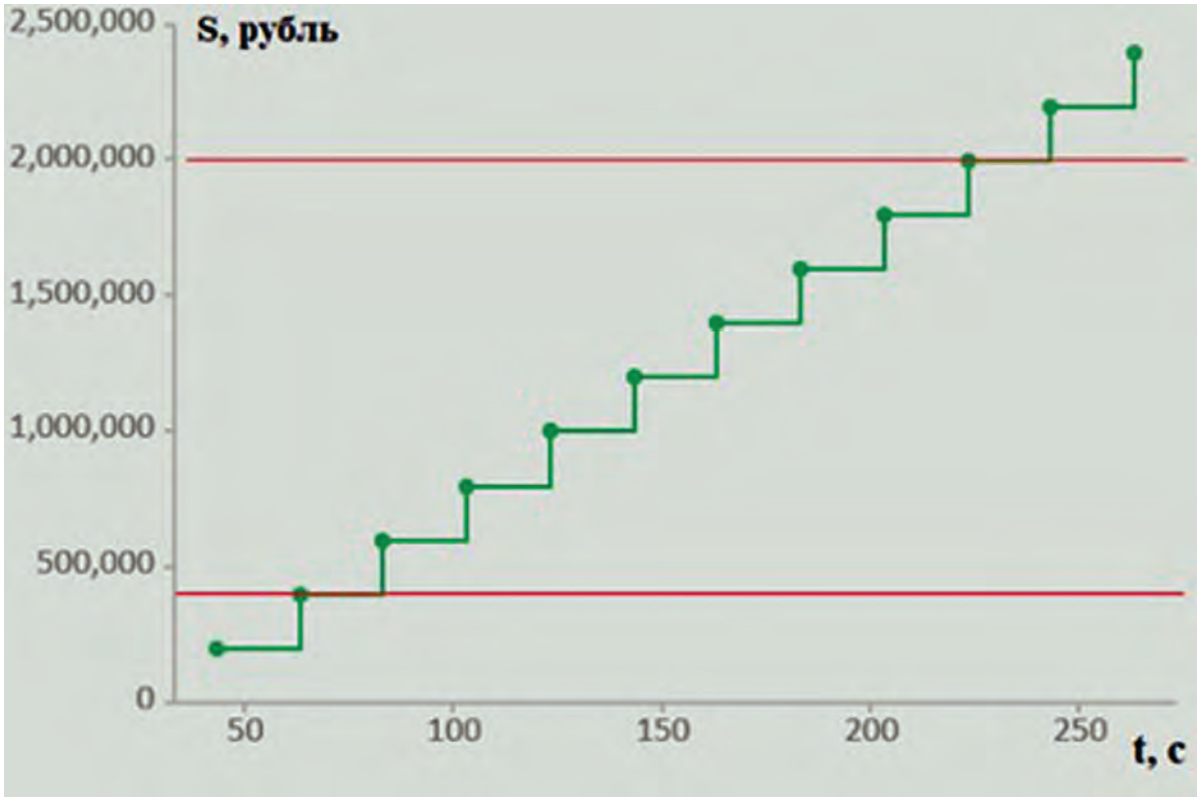


*Рис. 6. Взаимосвязь ущерба и времени приезда органов обеспечения правопорядка*

Исходя из расчётов, киберпреступник может извлечь от 200 000 до 2 000 000 руб. На рис. 6 показана зависимость суммы хищения от времени приезда правоохранительных органов, красными линиями обозначен промежуток максимальной и минимальной суммы в случае приезда наряда в промежутке от 4 до 7 минут. Если вскрытие сервисной зоны не было замечено, то сумма потерь составит ещё больше, вплоть до полного снятия доступных в сейфе средств.

Таким образом, при совершении атаки типа “Black box” нанесение ущерба возможно даже при незамедлительном реагировании на факт её возникновения. Это требует наличия систем мониторинга и индикаторов совершения операций, которые могут сигнализировать об атаке, но для полного предотвращения ущерба необходимо пресечь возможность злоумышленника начать использование ресивера банкомата в столь короткое время. Далее рассмотрим известные защитные меры от атак данного типа и предложим дополнительные методы защиты.

**Защитные меры от кибератак типа “Black box”**

Исходя из приведённых выше характеристик атаки и временны́х ограничений на её совершение, основными задачами службы безопасности банка будут являться:

1. Своевременное обнаружение факта подключения киберпреступника к системам банкомата;
2. Незамедлительное оповещение органов защиты правопорядка;
3. Блокировка изъятия наличных средств из сейфа.

Поскольку атаки данного типа выполняются напрямую на диспенсер, они эффективно изолируют мошенническую деятельность от традиционных средств защиты АТМ: систем авторизации транзакций и мониторинга. По этой причине обнаружение кибератак типа “Black box” в реальном времени может быть затруднено.

Для предотвращения атак, во время которых выполняется физическое вскрытие сейфовой зоны банкомата, можно использовать сигнализацию или отслеживание перехода банкомата в режим инкассации, но при совершении атаки типа “Black box” можно обнаружить лишь временное отключение диспенсера.

Возможность использования указанных событий в качестве индикаторов взлома также зависит от того, остаётся ли банкомат включённым и находится ли он в активном состоянии связи с системой удалённого мониторинга. Чтобы избежать обнаружения, киберпреступники иногда отключают АТМ перед началом атаки. Кроме того, некоторые устройства “Black box” требуют, чтобы банкомат был перезагружен, прежде чем киберпреступник сможет использовать устройство для управления диспенсером. Для обеспечения энергонезависимости банкоматов используются источники бесперебойного питания, поэтому АТМ, исчезающий из сети или неожиданно перезагружающийся, может использоваться как потенциальный метод обнаружения кибератаки.

В некоторых случаях сначала происходит установка устройства “Black box”, и только спустя некоторое время осуществляется изъятие денег из сейфа. Сотрудники, выполняющие обслуживание банкоматов, могут выпол-

нять осмотр на предмет наличия посторонней электроники или определить, не повреждены ли внутренние кабели. Данная мера позволяет предупредить ту часть атак, когда устройство устанавливается заранее для последующего удалённого использования.

Нередки случаи, когда возникают эксплуатационные проблемы, особенно когда выдаётся большое количество банкнот за короткий период времени. Например, диспенсер не может подобрать некоторые банкноты, и данное событие может быть зарегистрировано в журналах обслуживания АТМ. Сопоставление времени возникновения таких событий со временем совершения транзакций может использоваться для определения того, что диспенсер выдавал купюры в то время, когда никакие фактические транзакции не авторизовывались.

Таким образом, можно выделить перечень индикаторов, которые могут свидетельствовать о совершении атаки типа “Black box”:

1) открыта дверца сейфа банкомата (активирована тревога или режим инкассации);
2) модуль диспенсера удалён из списка доступных модулей;
3) перезагрузка системы АТМ, в том числе аварийное отключение системы, указывающее на то, что модуль был отключён;
4) банкомат отключился, а затем включился при работающем источнике бесперебойного питания;
5) отчёты о проверках сервисной зоны, отсутствие недоверенных электронных устройств и повреждённых кабелей;
6) проверка локальных журналов банкоматов, показывающих сбои подбора купюр или другие операционные ошибки диспенсера без соответствующих записей об авторизованных транзакциях по выдаче наличных.

Соблюдение указанных выше мер позволяет незамедлительно обнаружить атаку на банкомат, но не позволяет предотвратить её выполнение.

## Повышение эффективности реагирования и защиты банкоматов от атак типа “Black box”

Согласно рекомендациям производителей АТМ, предлагается использовать актуальные версии платформ XFS, обеспечивающие надёжное шифрование и поддерживающие физическую аутентификацию между ОС и диспенсером. При физической аутентификации ключи шифрования передаются только в случае подтверждения легальности доступа к сейфу. Указанные меры не гарантируют защищённость, например, имеет место случай, когда киберпреступникам удалось обойти физическую аутентификацию [17]. Также ненадёжность указанных методов подтверждается исследованиями компании Positive Technologies [11].

Существуют специальные устройства, обеспечивающие защиту от несанкционированного подключения к диспенсеру. Например, ЗУБ-Р, Cerber Lock и ATM Keeper. Они позволяют выполнять только аутентифицированные банковским ПО операции и расширить мониторинг событий безопасности банкомата. Основной проблемой данного способа противодействия кибератакам является малый процент банкоматов, использующий данные устройства. По данным компаний ООО «АНСЕР ПРО» и ООО «Artifakts» устройства используются в 15 000 АТМ, что составляет 7% от общего количества банкоматов [18, 19].

Вместе с тем в России до настоящего времени нет сколько-нибудь конкурентоспособного производства программно-технических средств связи и электронных компонентов [20] (не военных). Самые мощные вычислительные системы принадлежат Японии, США и Китаю. Японский суперкомпьютер «Фугаку» имеет пиковую производительность 537 петафлопс; российский «Кристофари» (принадлежит Сбербанку) – 8 петафлопс мощности[9].

Таким образом, перечисленные способы не обеспечивают надёжную защиту от атак типа “Black box”. Нужна разработка надёжного способа увеличить время, необходимое киберпреступнику для доступа к диспенсеру. Возможным способом будет являться установка временной задержки на запуск диспенсера после его включения. Минимальная продолжительность такой задержки равняется 217 сек. При использовании надёжных средств сигнализации это позволит сократить количество случаев успешной эксплуатации банкоматов методом “Black box”.

## Заключение

Рассмотренные меры направлены на повышение эффективности реагирования на инциденты информационной безопасности и, в частности, на развитие системы защиты клиентов от методов социальной инженерии и банкоматов от атак типа “Black box”. В работе обращается внимание на неразрывную связь стандартов по информационной безопасности и научных работ, направленных на решение задач кибербезопасности; проводится анализ кибератак на банкоматы типов “Brute force” и “Black box”. Научная новизна работы состоит в предложении авторами решения для ослабления приёмов социальной инженерии в результате сравнения их эффективности с эффективностью метода “Brute force”. Злоумышленнику проще подобрать «ключ» к человеческой логике, чем пароль или техническое устройство. Практическая значимость работы заключается в определении временны́х характеристик совершения атаки “Black box” и разработке дополнительных методов защиты банкоматов.

## Литература

1. Skinner Chris. Digital Human: The Fourth Revolution of Humanity Includes Everyone. Marshall Cavendish International (Asia) Pte Ltd, 2018. – 400 p.
2. Синки Дж. Финансовый менеджмент в коммерческом банке и в индустрии финансовых услуг. М.: Альпина Бизнес Букс, 2017. – 1018 с.

9 Писаренко Д. Россия в гонке вычислений. Почему по мощности суперкомпьютеров мы уступаем даже Саудовской Аравии? Еженедельник «Аргументы и Факты». 2021. № 8. С. 15. URL: https://aif.ru/society/science/gonka_vychisleniy_pochemu_nashi_superkompyutery_otstayut_ot_zarubezhnyh (дата обращения 04.03.2021).

3. Козьминых С.И. Методический подход к экономической оценке внедрения технических средств защиты информации в кредитно-финансовой организации // Вопросы кибербезопасности. 2020. № 3 (37). С. 87–96. DOI: 10.21681/2311-3456-2020-03-87-96.
4. Харрис Ш. Кибервойн@. Пятый театр военных действий. М.: Альпина нон-фикшн, 2016. – 390 с.
5. Зеленцов Б.П., Тутынина О.И. Теория вероятностей в познавательных и забавных задачах. М.: Книжный дом «Либроком», 2015. – 128 с.
6. Hadnagy C. Social Engineering: The Science of Human Hacking. Wiley publ., 2018. – 320 p.
7. Бердюгин А.А. Реинжиниринг бизнес-процессов коммерческого банка в информационном пространстве // Безопасность информационных технологий. 2021. Т. 28, №. 1, с. 62–73 DOI: 10.26583/bit.2021.1.05.
8. Россинская Е.Р., Рядовский И.А. Современные способы компьютерных преступлений и закономерности их реализации // Lex russica (Русский закон). 2019. № 3 (148). С. 87–99. DOI: 10.17803/1729-5920.2019.148.3.087-099.
9. Алексей Антонов. Как злоумышленники используют уязвимости АТМ // Расчеты и операционная работа в коммерческом банке. М.: Регламент, 2018. № 2 (144). С. 47–59. URL: http://futurebanking.ru/reglamentbank/article/4994 (дата обращения 23.02.2021).
10. Catalin Cimpanu. Diebold Nixdorf warns of a new class of ATM 'black box' attacks across Europe. Zero Day, 07.2020 URL: https://www.zdnet.com/article/diebold-nixdorf-warns-of-a-new-class-of-atm-black-box-attacks-across-europe/ (accessed on 10.03.2021).
11. Неваленный А.В., Ревенков П.В., Силин Н.Н., Фролов Д.Б. и др. Кибербезопасность в условиях электронного банкинга: практическое пособие / [Коллектив авторов, под ред. П.В. Ревенкова]. М.: Прометей; 2020. – 520 с.
12. Алексей Мальгавко. Эксперты в этом году наблюдают рост атак на банкоматы в России. АЭИ «ПРАЙМ», 10.2020. URL: https://1prime.ru/finance/20201027/832223407.html (дата обращения 10.03.2021).
13. Buldas A., Gadyatskaya O., Lenin A., Mauw S., Trujillo-Rasua R. Attribute evaluation on attack trees with incomplete information: a preprint. Computers & Security, 2020. Vol. 88. – 21 p. URL: https://arxiv.org/abs/1812.10754 (accessed on 28.02.2021).
14. Brian Krebs. Thieves Jackpot ATMS With 'Black Box' Attack. URL: https://krebsonsecurity.com/2015/01/thieves-jackpot-atms-with-black-box-attack (accessed on 10.02.2021).
15. Samuel Gibbs. Jackpotting: hackers are making ATMS give away cash. Guardian News, 01.2018. URL: https://www.theguardian.com/technology/2018/jan/29/jackpotting-hackers-atm-cash-machine-give-away (accessed on 24.03.2021).
16. Мария Воронова. Как можно незаметно потрошить банкоматы. URL: https://www.securitylab.ru/blog/company/infowatch/253888.php (дата обращения 27.02.2021).
17. Мария Нефёдова. Производитель банкоматов Diebold Nixdorf обнаружил новую форму атак в странах Европы, 07.2020. URL: https://xakep.ru/2020/07/17/new-jackpotting/ (дата обращения 28.02.2021).
18. Barabanov A., Markov A., Tsirlov V. On systematics of the information security of software supply chains // Advances in Intelligent Systems and Computing (см. в книгах). 2020. Т. 1294. Pp. 115–129. DOI: 10.1007/978-3-030-63322-6_9.
19. Киздермишов А.А. Анализ возможности использования свободно распространяемых сетевых сканеров // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. 2014. № 3 (142). С. 201–205. URL: https://www.elibrary.ru/item.asp?id=23055763 (дата обращения 24.02.2021).
20. Гущина Е.А., Макаренко Г.И., Сергин М.Ю. Обеспечение информационно-технологического суверенитета государства в условиях развития цифровой экономики // Право.by. 2018. № 6 (56). С. 59–63.

# ASSESSMENT OF THE RISK OF A CYBERSECURITY BREACH IN A COMMERCIAL BANK (BY THE EXAMPLE OF AN ATTACKS "BRUTE FORCE" AND "BLACK BOX" ON ATMS)

***Revenkov P.V.[10], Berdyugin A.A.[11], Makeev P.V.[12]***

***Abstract.*** *During the XX–XXI century there was a development of technologies, which resulted in the creation of a global financial system that allows you to quickly make money transactions in opposite points of the Earth. The progress of digital transformation of society and, in particular, financial and economic systems leads to the complication of the*

10 Pavel Revenkov, Dr.Sc., Assistant Professor, Professor of the Department of Information Security, Financial University under the Government of the Russian Federation, Moscow, Russia. E-mail: pavel.revenkov@mail.ru, orcid.org/0000-0002-0354-0665

11 Alexander Berdyugin, Junior researcher of the Department of Information Security, Financial University under the Government of the Russian Federation, Moscow, Russia. E-mail: brdgn@bk.ru, orcid.org/0000-0003-2301-1776

12 Pavel Makeev, Master's Degree student of the Faculty of Information Technology and Big Data Analysis, Financial University under the Government of the Russian Federation, Moscow, Russia. E-mail: paulmakeev@gmail.com, orcid.org/0000-0003-0031-5419

*problems of information security of competing entities. By focusing on scientific research, we can achieve success in these areas.*

***The purpose of the study:*** *to increase the level of security of banking services for individuals and legal entities in accordance with the recommendations of information security standards by analyzing the risk of information security violations in electronic banking technologies (on the example of the "Brute force" and "Black box" attacks).*

***Research methods:*** *empirical methods of scientific knowledge (observation, measurement, experiment), theoretical methods (analysis, synthesis, induction, deduction, abstraction, formalization), graphical interpretation of information, probability theory methods and computer programming.*

***The result of the study:*** *standards for effective management of information security management at the enterprise are considered. The advantage of social engineering methods over the "Brute force" method of PIN codes is shown quantitatively. The time characteristics of its commission and protective measures against attacks of the "Black box" type are analyzed. A method for improving the effectiveness of the response and protection of ATMS from attacks of the "Black box" type is proposed.*

***Keywords:*** *standards, PIN code, probability of selection, ATM, dispenser, cybercriminal, duration of a cyberattack.*

## References

1. Skinner Chris. Digital Human: The Fourth Revolution of Humanity Includes Everyone. Marshall Cavendish International (Asia) Pte Ltd, 2018. – 400 p.
2. Sinki Dzh. Finansovyy menedzhment v kommercheskom banke i v industrii finansovykh uslug. M.: Al'pina Biznes Buks, 2017. – 1018 s.
3. Kozminykh S.I. Metodicheskiy podkhod k ekonomicheskoy otsenke vnedreniya tekhnicheskikh sredstv zashchity informatsii v kreditno-finansovoy organizatsii // Voprosy kiberbezopasnosti. 2020. № 3 (37). S. 87–96. DOI: 10.21681/2311-3456-2020-03-87-96.
4. Harris Sh. Kibervoyn@. Pyatyy teatr voyennykh deystviy. M.: Al'pina non-fikshn, 2016. – 390 s.
5. Zelentsov B.P., Tutynina O.I. Teoriya veroyatnostey v poznavatel'nykh i zabavnykh zadachakh. M.: Knizhnyy dom «Librokom», 2015. – 128 s.
6. Hadnagy C. Social Engineering: The Science of Human Hacking. Wiley publ., 2018. – 320 p.
7. Berdyugin A.A. Reinzhiniring biznes-protsessov kommercheskogo banka v informatsionnom prostranstve // Bezopasnost' informatsionnykh tekhnologiy. 2021. T. 28, №. 1, s. 62–73 DOI: 10.26583/bit.2021.1.05.
8. Rossinskaya E.R., Ryadovskiy I.A. Sovremennyye sposoby komp'yuternykh prestupleniy i zakonomernosti ikh realizatsii // Lex russica (Russkiy zakon). 2019. № 3 (148). S. 87–99. DOI: 10.17803/1729-5920.2019.148.3.087-099.
9. Aleksey Antonov. Kak zloumyshlenniki ispol'zuyut uyazvimosti ATM // Raschety i operatsionnaya rabota v kommercheskom banke. M.: Reglament, 2018. № 2 (144). S. 47–59. URL: http://futurebanking.ru/reglamentbank/article/4994 (data obrashcheniya 23.02.2021).
10. Catalin Cimpanu. Diebold Nixdorf warns of a new class of ATM 'black box' attacks across Europe. Zero Day, 07.2020 URL: https://www.zdnet.com/article/diebold-nixdorf-warns-of-a-new-class-of-atm-black-box-attacks-across-europe/ (accessed on 10.03.2021).
11. Nevalennyy A.V., Revenkov P.V., Silin N.N., Frolov D.B. i dr. Kiberbezopasnost' v usloviyakh elektronnogo bankinga: prakticheskoye posobiye / [Kollektiv avtorov, pod red. P.V. Revenkova]. M.: Prometey; 2020. – 520 s.
12. Alexey Malgavko. Eksperty v etom godu nablyudayut rost atak na bankomaty v Rossii. AEI «PRAYM», 10.2020. URL: https://1prime.ru/finance/20201027/832223407.html (data obrashcheniya 10.03.2021).
13. Buldas A., Gadyatskaya O., Lenin A., Mauw S., Trujillo-Rasua R. Attribute evaluation on attack trees with incomplete information: a preprint. Computers & Security, 2020. Vol. 88. – 21 p. URL: https://arxiv.org/abs/1812.10754 (accessed on 28.02.2021).
14. Brian Krebs. Thieves Jackpot ATMS With 'Black Box' Attack. URL: https://krebsonsecurity.com/2015/01/thieves-jackpot-atms-with-black-box-attack (accessed on 10.02.2021).
15. Samuel Gibbs. Jackpotting: hackers are making ATMS give away cash. Guardian News, 01.2018. URL: https://www.theguardian.com/technology/2018/jan/29/jackpotting-hackers-atm-cash-machine-give-away (accessed on 24.03.2021).
16. Mariya Voronova. Kak mozhno nezametno potroshit' bankomaty. URL: https://www.securitylab.ru/blog/company/infowatch/253888.php (data obrashcheniya 27.02.2021).
17. Mariya Nefedova. Proizvoditel' bankomatov Diebold Nixdorf obnaruzhil novuyu formu atak v stranakh Yevropy, 07.2020. URL: https://xakep.ru/2020/07/17/new-jackpotting/ (data obrashcheniya 28.02.2021).
18. Barabanov A., Markov A., Tsirlov V. On systematics of the information security of software supply chains // Advances in Intelligent Systems and Computing (sm. v knigakh). 2020. T. 1294. Pp. 115–129.
19. Kizdermishov A.A. Analiz vozmozhnosti ispol'zovaniya svobodno rasprostranyayemykh setevykh skanerov // Vestnik Adygeyskogo gosudarstvennogo universiteta. Seriya 4: Yestestvenno-matematicheskiye i tekhnicheskiye nauki. 2014. № 3 (142). S. 201–205. URL: https://www.elibrary.ru/item.asp?id=23055763 (data obrashcheniya 24.02.2021).
20. Gushchina E.A., Makarenko G.I., Sergin M.Y. Obespecheniye informatsionno-tekhnologicheskogo suvereniteta gosudarstva v usloviyakh razvitiya tsifrovoy ekonomiki // Pravo.by. 2018. № 6 (56). S. 59–63.