ОРИГИНАЛЬНАЯ СТАТЬЯ

DOI: 10.26794/2587-5671-2020-24-6-51-60
УДК 004.056:336(045)
JEL G21, G32, L86

Оценка риска воздействия кибератак в технологиях электронного банкинга (пример программной реализации)

А.А. Бердюгин[a], П.В. Ревенков[b]
Финансовый университет, Москва, Россия
[a] https://orcid.org/0000-0003-2301-1776; [b] https://orcid.org/0000-0002-0354-0665

АННОТАЦИЯ

Авторы исследуют риски компьютерных атак на автоматизированные банковские системы. **Актуальность** исследования обусловлена необходимостью пересмотра подходов к оценке рисков, в основе которых лежат технические составляющие банковских бизнес-процессов и последствия кибератак, направленных на банковские автоматизированные системы в кредитных организациях. **Цель** исследования состоит в описании разработанных методов оценки киберриска в коммерческом банке и предложении одного из вариантов оценки рисков нарушения информационной безопасности в технологиях электронного банкинга. **Методология** статьи включает анализ отечественной и зарубежной литературы по теме исследования, теоретико-вероятностный метод расчета, компьютерное программирование и графическую интерпретацию информации. Проанализирован операционный риск коммерческого банка для разработки компонентов системы операционного риск-менеджмента в условиях развития технологий электронного банкинга. Разработана компьютерная программа для количественной оценки вероятности риска воздействия кибератак на технологии электронного банкинга (с использованием Borland Delphi). Формализована вероятностная модель определения наиболее уязвимого сегмента техник риск-менеджмента, используемых структурами по обеспечению информационной безопасности. Сделан **вывод** о возможности разработки программного комплекса на основании математической модели, позволяющей сократить количество проверок факторов риска в несколько раз. **Результаты** исследования могут быть применены для дальнейших практических разработок риск-подразделений кредитных организаций, использующих технологии электронного банкинга.

Ключевые слова: риск воздействия кибератак; технологии электронного банкинга; информационная безопасность; оценка риска; вероятностная модель; компьютерная программа; типичные банковские риски

Для цитирования: **Бердюгин А.А., Ревенков П.В. Оценка риска воздействия кибератак в технологиях электронного банкинга (пример программной реализации).** ***Финансы: теория и практика.*** **2020;24(6):51-60. DOI: 10.26794/2587-5671-2020-24-6-51-60**

ORIGINAL PAPER

Cyberattack Risk Assessment in Electronic Banking Technologies (the Case of Software Implementation)

A.A. Berdyugin[a], P.V. Revenkov[b]
Financial University, Moscow, Russia
[a] https://orcid.org/0000-0003-2301-1776; [b] https://orcid.org/0000-0002-0354-0665

ABSTRACT

The authors investigate the risks of computer attacks on automated banking systems. **The relevance** of the study is due to the need to revise the approaches to risk assessment based on the technical components of banking business processes and the consequences of cyber-attacks aimed at banking automated systems in credit institutions. **The aim** of the study is to describe the developed methods for assessing cyber risks in a commercial bank and provide an option for assessing the risks of information security violations in electronic banking technologies. **The methodology** of the article includes the analysis of domestic and foreign literature on the research topic, the theoretical and probabilistic method of calculation, computer programming and graphic interpretation of information. The authors analysed the operational risk of a commercial bank to develop components of the operational risk management system in the context of developing

electronic banking technologies. They designed a computer program to quantify risk probabilities of cyberattacks on electronic banking technologies (by means of Borland Delphi). The work presents a formalised probabilistic model for determining the most vulnerable segment of risk management techniques used by information security structures. **The conclusion** is that it is possible to develop a software package based on a mathematical model that reduces the number of checks of risk factors by several times. **The research results** may be of further use for the development of risk divisions in credit institutions using electronic banking technologies.
Keywords: the risk of cyberattacks; electronic banking technologies; information security; risk assessment; probabilistic model; computer program; typical banking risks

For citation: **Berdyugin A.A., Revenkov P.V. Cyberattack risk assessment in electronic banking technologies (the case of software implementation).** ***Finance: Theory and Practice*****. 2020;24(6):51-60. (In Russ.). DOI: 10.26794/2587-5671-2020-24-6-51-60**

ВВЕДЕНИЕ

Научно-технический прогресс способствует переходу традиционного банковского обслуживания в дистанционный формат и расширению профилей рисков. По мнению ряда экспертов (например, B. King [1] и C. Skinner [2]), в 2020-х гг. в мире появятся страны, которые полностью откажутся от наличных денег (Швеция, Китай, Канада).

Первым в России примером использования технологии smart card стал моногород Нерюнгри (Якутия), продемонстрировавший потенциал безналичных расчетов будущего. Перестройка СССР стала причиной проблем с наличностью. Градообразующее предприятие «Якутуголь» (сегодня дочерняя организация «Мечела») выдавало зарплаты рабочим качественной техникой из Японии (бартер), а в 1995 г. при помощи основного в городе «Нерюнгрибанка» (сейчас «Углеметбанк») перевело зарплаты всех своих сотрудников на пластиковые карты «Золотая корона» [3].

Разработка новосибирского «Центра финансовых технологий» опережала время и оказалась удобной для всех профессий и слоев населения, включая пенсионеров[1]. Один из авторов данной статьи (А. А. Бердюгин) стал очевидцем этих нововведений, потому что родился и проживал в городе Нерюнгри с 1988 по 2010 г. до переезда в Москву. Постепенный отказ от наличных денег является следствием активного внедрения технологий электронного банкинга (ТЭБ)[2] в банковский бизнес [4] и предоставляет шанс (противоположное риску событие) для киберпреступников.

Наряду с очевидными преимуществами ТЭБ, значительно расширились профили типичных банковских рисков, среди которых особо можно выделить операционный риск (ОР). Базельский комитет по банковскому надзору, являясь одним из ведущих разработчиков методологии оценки банковских рисков в мире, выпустил несколько документов по совершенствованию банковского надзора, в которых рекомендует кредитным организациям формировать резерв под операционный риск, в который включается резерв и под киберриск (см. комплексы документов Базель II, III и IV)[3].

В соответствии с рекомендациями комитета коммерческим банкам необходимо резервировать средства под ОР, учитывая также активное развитие и использование информационных технологий (финтех или техфин [1, 2]).

Под ОР понимается риск возникновения прямых и косвенных потерь в результате:

- низкой эффективности или ошибочных внутренних бизнес-процессов коммерческого банка;
- действий служебного персонала и сторонних лиц;
- нарушений и недостатков в работе информационных, технологических и других систем;
- внешних событий.

ОР включает в себя правовые риски, но исключает стратегические и репутационные риски. Также сюда входят различные виды рисков в зависимости от видов процессов:

- риск недостаточного обеспечения информационной безопасности;

[1] Искусство выживания: что помогло ЦФТ преодолеть все финансовые кризисы. URL: https://www.rbc.ru/magazine/2016/12/582c40a29a7947079b45fdce (дата обращения: 26.05.2020).

[2] Основу ТЭБ составляют PC-banking (управление банковскими счетами и картами с компьютера через интернет и Web-браузер в режиме онлайн) и мобильный банкинг (SMS-banking, а также управление банковскими счетами и картами через специальное приложение со смартфонов, планшетов и smart-часов). К ТЭБ относятся также банкоматы и терминалы банковского самообслуживания.

[3] С содержанием данных документов, а также с различными статьями ведущих экспертов в области банковского надзора можно познакомиться на сайте bis.org.

Рис. 1 / Fig. 1. **Построение системы управления ОР в условиях применения ТЭБ / Building an operational risk management system in the context of electronic banking technologies**

Источник / Source: составлено авторами на основе [5] / complied by the authors based on [5].

- риск, связанный с недостатками в построении информационных систем в конкретной организации;
- проектный риск как следствие проявления источников ОР;
- риск нарушения процедур контроля, который может включать комплаенс-риск или риск недостатков внутреннего контроля;
- риск ошибок процессов разработки, проверки, адаптации, приемки методик и количественных моделей оценки активов и рисков (модельный риск как следствие проявления источников ОР);
- риск, связанный с ошибочными действиями персонала организации.

В целом система управления ОР в условиях применения ТЭБ может выглядеть следующим образом (*рис. 1*) [5]. Адаптируя общепринятый термин «риск нарушения информационной безопасности» к статье, рассмотрим проявления ОР в ТЭБ.

Определение 1. Под риском воздействия кибератак (РВКа) будем понимать количественное выражение вероятности возрастания типичных банковских рисков под влиянием инсайдерских и хакерских угроз, при нарушениях работы автоматизированной банковской системы, а также выражение величины отрицательных последствий (финансовые издержки, снижение репутации, потеря ликвидности), причиной которых стала реализация угрозы. Понятие РВКа в ТЭБ использовано авторами в [3, 6, 7].

Ключевым для системы управления ОР является программный комплекс, обеспечивающий ее функционирование в условиях применения ТЭБ. Подверженные кибератакам ТЭБ можно классифицировать по способу предоставления финансовых дистанционных услуг:

- PC-banking;
- Telephone/SMS banking;
- Terminal banking;
- Mobile banking.

Тестирование на проникновение в защищаемый периметр коммерческих банков, проведенное экспертами Positive Technologies, показало, что у семи из восьми организаций локальная сеть не защищена от проникновения из глобальной сети. Защищенность корпоративной инфраструк-

туры большинства рассмотренных кредитно-финансовых организаций от внутренних кибератак оценена компанией как крайне низкая[4]. При этом коммерческие банки возместили своим клиентам только 15% (935 млн руб., или каждый седьмой похищенный рубль), объясняя это высокой долей социальной инженерии: клиенты сами раскрывают конфиденциальную информацию[5].

Таким образом, кибератаки несут значительный ущерб для банков и становятся причиной реализации типичных банковских рисков (кредитный, операционный, правовой, репутационный, стратегический риски и риск ликвидности), характеристика которых приведена в письме Банка России № 70-Т «О типичных банковских рисках»).

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ МЕТОДА ОЦЕНКИ РВКа В ТЭБ

Согласно Федеральному закону Российской Федерации № 184-ФЗ «О техническом регулировании», риск — это вероятность причинения вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений с учетом тяжести этого вреда [6]. В *табл. 1* приведена сравнительная характеристика программных средств для оценки рисков воздействия кибератак.

Как видим, отечественное программное обеспечение для оценки рисков ограничивается продуктом «ГРИФ 2006», который не поддерживается производителем. Поэтому автоматизируем метод количественной оценки менеджмента РВКа в ТЭБ, приведенный в работах авторов [3, 6], на языке высокого уровня (ЯВУ) Borland Delphi (интуитивно понятный интерфейс и готовый пример см. на *рис. 2*) с применением [9–11].

1. Вначале риск-аналитик выбирает вопрос-требование из ниспадающего списка и оценивает его четырьмя переключателями (примерный ряд требований, предъявляемых к системе управления РВКа приведен в [3, 6]), задавая тем самым исходные данные:

```
...
Cells[1, Row]:= IntToStr(RadioGroup.
ItemIndex + 1);
...
```

2. После заполнения ячеек вопросами-требованиями и их оценки по 4-балльной шкале определяется количественное значение вероятности неблагоприятного исхода при реализации РВКа нажатием на кнопку «Вероятность РВКа»:

```
procedure TRiskForm.
ProbabilityButtonClick(Sender:
TObject);
var
  znam, j: Integer;
begin
  znam:= 0;
  for j:= 1 to
  ConditionOfBankStringGrid.rowCount
  do
    if ConditionOfBankStringGrid.
    Cells[1, j] <> '' then
  begin
    znam:= znam + StrToInt(Conditio
    nOfBankStringGrid.Cells[1, j]);
    // Cells[Col, Row]
    ProbabilityLabel.Caption:=
    FloatToStr(SimpleRoundTo(100 * j /
    znam,—2)) + '%';
    RadioGroup.ItemIndex:= -1; // чтобы
    снимались переключатели
  end;
end;
```

Выполнение требования (положительный ответ) уменьшает процент (вероятность) РВКа и наоборот.

3. Для дальнейшей работы требования и расчеты могут быть сохранены в отчет Microsoft Excel нажатием на соответствующую кнопку:

```
...
  with ConditionOfBankStringGrid do
  begin
    for i:= 0 to ColCount — 1 do
      for j:= 0 to RowCount — 1 do
      Excel.Sheets[1]. Cells [j + 1, i +
      1]:= Cells [i, j]; // "Связать"
      Excel и Delphi
  end;
    Excel.Sheets[1]. Cells [1, 7]:=
   'Итог: '; {Записываем процент РВКа}
    Excel.Sheets[1]. Cells [1, 8]:=
    ProbabilityLabel.Caption;
```

[4] Тестирование на проникновение в организациях кредитно-финансового сектора. URL: https://www.ptsecurity.com/ru-ru/research/analytics/pentest-finance-2020/ (дата обращения: 27.06.2020).

[5] Отчет Банка России «Обзор операций, совершенных без согласия клиентов финансовых организаций за 2019 год». URL: http://www.cbr.ru/Content/Document/File/103609/Review_of_transactions_2019.pdf (дата обращения: 28.06.2020).

Таблица 1 / Table 1

Сравнительная характеристика средств оценки рисков воздействия кибератак / Comparative characteristics of cyberattack risk assessment tools

Продукт / Product:	CRAMM (Central Computer Telecommunications Agency, UK)	RiskWatch, компания RiskWatch (USA)	ГРИФ 2006, компания Digital Security Office (Россия) / GRIF 2006, Digital Security Office (Russia)	Microsoft Security Assessment Tool
Поддержка:	Обеспечивается	Обеспечивается	Отсутствует	Обеспечивается
Легкость в работе конечного пользователя:	Требует специальной подготовки и высокой квалификации аудитора	Требует специальной подготовки и высокой квалификации аудитора	Интерфейс программы ориентирован на IT-менеджеров и руководителей. Требует специальных знаний в области информационной безопасности	Интерфейс программы ориентирован на IT-менеджеров и руководителей. Требует специальных знаний в области информационной безопасности
Цена:	Стоимость лицензии от 2 тыс. до 5 тыс. долл. за одно рабочее место	Стоимость лицензии от 10 тыс. долл. за одно рабочее место	Стоимость лицензии от 1 тыс. долл. за одно рабочее место	Бесплатно
Входные данные:	– Ресурсы; – ценность ресурсов; – угрозы; – уязвимости системы; – выбор адекватных мер	– Тип информационной системы; – базовые требования в области безопасности; – ресурсы; – потери; – угрозы; – уязвимости; – меры защиты; – ценность ресурсов; – частота возникновения угроз; – выбор контрмер	– Ресурсы; – сетевое оборудование; – виды информации; – группы пользователей; – средства защиты; – угрозы; – уязвимости; – выбор контрмер	Формируются на основе ответов пользователя
Варианты/состав отчета:	– Отчет по анализу рисков; – общий отчет по анализу рисков; – детализированный отчет по анализу рисков	– Краткие итоги; – отчет о стоимости защищаемых ресурсов и ожидаемых потерь от реализации угроз; – отчет об угрозах и мерах противодействия; – отчет об убыточности бизнеса; – отчет о результатах аудита безопасности	– Инвентаризация ресурсов; – риски по видам информации; – риски по ресурсам; – соотношение ущерба от РВКа и ресурса; – выбранные контрмеры; – рекомендации экспертов	– Подробное руководство; – рекомендации по снижению уровня РВКа; – ссылки на отраслевые руководства; – профиль банковского риска; – индекс глубокой защиты
Количественный или качественный метод:	Качественная оценка	Количественная оценка	Качественная и количественная оценка	Качественная оценка
Наличие сетевого решения:	Отсутствует	Отсутствует	Корпоративная версия	Отсутствует

Источник / Source: составлено на основе работ авторов [8] / compiled based on the works of the authors [8].

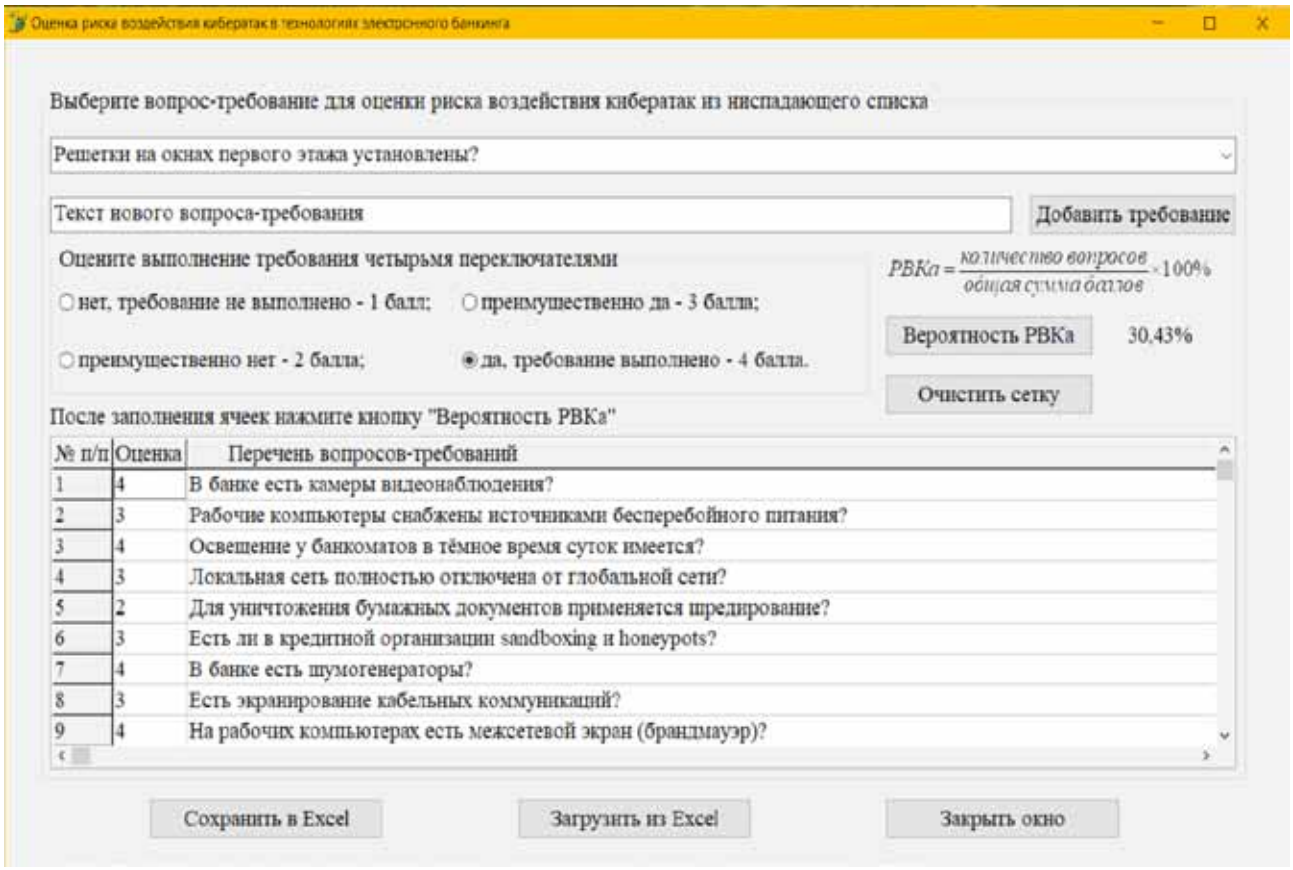

Рис. 2 / Fig. 2. **Пример использования программы, оценивающей РВКа / Example of using the program that assesses the risks of cyberattacks**

Источник / Source: разработано авторами на ЯВУ Delphi / developed by the authors in the high-level language Borland Delphi.

```
  Excel.DisplayAlerts:= False; // От-
  ключаем предупреждения Excel
  if SaveDialog.Execute then // Если
  запустили окно сохранения, то
  try
    Excel.ActiveWorkbook.
    SaveAs(SaveDialog.FileName);
    ShowMessage ('Сохранено в файл: '
    + #10 + SaveDialog.FileName);
  except
    ShowMessage ('Невозможно сохра-
    нить файл, он открыт для записи
    или доступен только для чтения.'
    + #10 + 'Попробуйте сохранить
    файл под другим именем.');
  end;
```

...

4. Имеющийся перечень требований и оценок можно загрузить из базы Excel:

...

```
  Excel:= CreateOleObject ('Excel.
  Application');
  Excel.Workbooks.Open(OpenDialog.
  FileName);
  with ConditionOfBankStringGrid do
  begin
    for i:= 2 to Excel.ActiveSheet.
    UsedRange.Rows.Count do
    for j:= 1 to ColCount do
    begin
      {Кол-во строк (рядов) StringGrid
      делаем равным количеству …}
      RowCount:= Excel.ActiveSheet.
      UsedRange.Rows.Count; {…заполнен-
      ных строк Excel}
      Cells [j-1, i-1]:= Excel.
      Sheets[1]. Cells [i, j]; {Загру-
      зить из Excel в Delphi}
    end;
  end;
```

...

Перечень вопросов-требований разработан авторами исследования эмпирическим путем и на основе анализа соответствующей литературы. Его доработка возможна при производственной эксплуатации программы.

5. Программа работает при подключении соответствующих модулей:

```
uses
...
  Math {подключаем модуль работы с ма-
  тематическими функциями},
  ComObj {подключаем модуль работы
  с COM-объектами Microsoft};
...
var
  RiskForm: TRiskForm;
  Excel: OleVariant; {Объявление объекта
  OleVariant с именем Microsoft Excel}
...
```

Примечание. В программе предусмотрено, чтобы вероятность реализации риска не была равна нулю, так как абсолютной защиты не существует. Отличительной особенностью ЯВУ Delphi является необходимость отключения реакции Delphi на исключительные ситуации (try — except — end): в пункте системного меню Tools → Debugger Options → Language Exceptions → отключить Stop on Delphi Exceptions[6].

Регулярное применение программы структурами по обеспечению кибербезопасности коммерческого банка позволит вести мониторинг эффективности мер, которые направлены на нивелирование негативных последствий реализации РВКа в условиях применения ТЭБ. Итоговая оценка вероятности РВКа позволяет получить представление о защищенности корпоративной инфраструктуры кредитной организации. Во введении статьи защищенность большинства банков описана как крайне низкая (см. выше результаты Positive Technologies о тестировании на проникновение). Использование разработанной программы для оценки РВКа в условиях применения ТЭБ позволит эффективно управлять общей системой риск-менеджмента в кредитной организации.

РАЗРАБОТКА ВЕРОЯТНОСТНОЙ МОДЕЛИ ОЦЕНКИ РВКа В ТЭБ

Хищение крупных сумм электронных денежных средств включает в себя не только кражу номеров и PIN-кодов банковских карт или паролей доступа к банковским счетам, но и разработку механизма вывода краденых денег на «безопасные» счета (речь идет о так называемом процессе легализации денежных средств). Делается это различными способами: через последовательность электронных перечислений в ТЭБ жертвы на счета злоумышленника с привлечением подставных лиц или путем приобретения товаров в online-магазинах с последующей их перепродажей по сниженным ценам [12–14].

Для более детального анализа авторами разработан метод, при котором количество проверок факторов риска[7], способствующих хищению и выводу денежных средств, при общем количестве n негативных факторов, может быть уменьшено в несколько раз следующим образом:

Тестирование на проникновение в защищаемый периметр коммерческих банков, проведенное экспертами Positive Technologies, показало, что у семи из восьми организаций локальная сеть не защищена от проникновения из глобальной сети.

1. Предположительные потери денег суммируются в группы по k факторов РВКа $(k<n)$.
2. Размер возможных потерь, попадающий в интервал незначительных или допустимых рисков, предполагает завершение цикла.
3. Размер возможных потерь, попадающий в интервал критических или катастрофических рисков, требует отдельного рассмотрения каждого из n факторов. Тогда для k факторов РВКа требуется провести $k+1$ проверку.

Доказательство. Составим вероятностную модель оценки РВКа в ТЭБ, которая может стать основой для методов, разрабатываемых в [15]. Пусть вероятность критических или катастрофических потерь равна p и одинакова для каждого из n факторов. Потери от реализации РВКа в ТЭБ для каждого фактора независимы. Элементы вероятностной модели составляют последовательность из распределений Бернулли для n испытаний с вероятностью p.

Определение 2. Распределение Бернулли моделирует случайный эксперимент произволь-

[6] Codecall Programming Forum. Community Forum Software by IP.Board. URL: http://forum.codecall.net (дата обращения: 10.07.2020).

[7] Под факторами риска понимается количественное выражение исполнения вопросов-требований из предыдущего раздела.

ной природы при заранее известной вероятности успеха или неудачи. Случайная величина ς имеет распределение Бернулли с вероятностью $p\left(0 \le p \le 1\right)$, если принимаемые ею значения равны 0 или 1 с вероятностями $P\left(\varsigma = 0\right) = 1 - p$ и $P\left(\varsigma = 1\right) = p$ соответственно.

Предположим, что n делится нацело на k. Проверке подвергнутся n/k групп факторов. Пусть X_j – число проверок, выполненных в j-й группе, $j = 1, 2, \ldots, n/k$. Тогда

$$X_j = \begin{cases} 1, \text{с вероятностью } P\left(X_j\right) = \left(1-p\right)^k, \\ \text{все } k \text{ факторов в пределах нормы} \\ k+1, \text{с вероятностью } P\left(X_j\right) = 1-\left(1-p\right)^k, \\ \text{есть негативные факторы.} \end{cases}$$

Здесь $\left(1-p\right)^k$ является произведением (совмещением) событий, противоположных критическим или катастрофическим потерям. Пусть $Z = X_1 + X_2 + \ldots + X_{n/k}$ – это общее число проверок. Оценим размер группы $k_0 = k_0\left(p\right)$ для заданного значения p (значение p можно оценить с помощью частоты обнаружения негативных факторов в предыдущих испытаниях). Этот размер группы $k_0 = k_0\left(p\right)$ должен минимизировать величину математического ожидания $M\left(Z\right)$. Согласно определению математического ожидания $M\left(\xi\right) = \sum_k x_k p_k$ находим:

$$M\left(X_j\right) = 1 \cdot \left(1-p\right)^k + \left(k+1\right) \cdot \left[1 - \left(1-p\right)^k\right] = \\ = k + 1 - k \cdot \left(1-p\right)^k.$$

Из свойства математического ожидания $M\left(\xi + \eta\right) = M\left(\xi\right) + M\left(\eta\right)$ имеем:

$$M\left(Z\right) = M\left(X_1\right) + M\left(X_2\right) + \ldots + M\left(X_{n/k}\right) = \\ = \frac{n}{k} \cdot M\left(X_j\right) = n \cdot \left[1 + 1/k - \left(1-p\right)^k\right].$$

Определению размера группы $k_0 = k_0\left(p\right)$ способствует предположение, что $H\left(x\right) = 1 + 1/x - \left(1-p\right)^x$ при $x > 0$. Для значений p, которые близки к 0, функция $H\left(x\right)$ достигнет минимума в точке x_0, являющейся минимальным экстремумом уравнения $H'\left(x\right) = 0$, т.е.

$$\left[1 + 1/x - \left(1-p\right)^x\right]' = 1/x^2 + \left(1-p\right)^x \cdot \ln\left(1-p\right).$$

Получившееся уравнение относительно x явно не разрешимо. По формуле бинома Ньютона при малых p имеем $\left(1-p\right)^x \approx 1 - px$. Сделав замену

$$H\left(x\right) = 1 + 1/x - \left(1-p\right)^x$$

на $\tilde{H}\left(x\right) = 1 + 1/x - 1 + px = 1/x + px$, найдем точку минимума функции:

$$\left(1/x + px\right)' = 0 \Leftrightarrow -1/x^2 + p = 0,$$

откуда $\tilde{x}_0 = 1/\sqrt{p}$.

При этом $\tilde{H}\left(\tilde{x}_0\right) = \sqrt{p} + p/\sqrt{p} = 2\sqrt{p}$. Пусть минимальная вероятность критических или катастрофических потерь равна 1%. Тогда для $p = 0{,}01$ получаем:

$$\tilde{x}_0 = 1/\sqrt{0{,}01} = 10, \quad \tilde{H}\left(\tilde{x}_0\right) = 2\sqrt{0{,}01} = 1/5,$$

$$M\left(Z\right) \approx n \cdot \tilde{H}\left(\tilde{x}_0\right) = n/5.$$

Дальнейшие исследования авторов позволят разработать программный комплекс для автоматизации выявления факторов риска, что сократит количество проверок в несколько раз.

Ожидаемое количество проверок потерь $M\left(Z\right) = n/5$ (пятикратное сокращение). Предложенная для выявления негативных факторов риска модель позволяет уменьшить в 5 раз время, затраченное на проведение проверок денежных потерь от реализации РВКа, благодаря чему значительно повышается эффективность мер определения наиболее уязвимого сегмента, используемых структурами обеспечения информационной безопасности техник менеджмента РВКа.

ВЫВОДЫ

Дальнейшие исследования авторов позволят разработать программный комплекс для автомати-

зации выявления факторов риска, что сократит количество проверок в несколько раз.

Внедрение ТЭБ способствует значительному сокращению затрат кредитных организаций на операционные расходы, но при этом работа банка в киберпространстве сопряжена с дополнительными источниками типичных банковских рисков.

Авторами предложен достаточно простой способ оценки РВКа, который при необходимости может постоянно расширяться за счет включения дополнительных параметров контроля и разработки новых моделей. Его можно использовать на постоянной основе специалистами риск-подразделений. Результаты оценки РВКа могут повысить эффективность решений, принимаемых кредитными организациями для обеспечения кибербезопасности в условиях применения ТЭБ.

СПИСОК ИСТОЧНИКОВ

1. King B. Bank 4.0: Banking everywhere, never at a bank. Singapore: John Wiley & Sons Ltd; 2018. 352 p.
2. Skinner C. Digital human: The fourth revolution of humanity includes everyone. Singapore: Marshall Cavendish International (Asia) Pte Ltd; 2018. 400 p.
3. Ревенков П.В., Бердюгин А.А. Метод количественной оценки риска воздействия кибератак в условиях электронного банкинга. *Банковское дело*. 2020;7:32–37.
4. Salihu A., Metin H., Hajrizi E., Ahmeti M. The effect of security and ease of use on reducing the problems/deficiencies of Electronic Banking Services. *IFAC-PapersOnLine*. 2019;52(25):159–163. DOI: 10.1016/j.ifacol.2019.12.465
5. Kleijmeer R., Prenio J., Yong J. Varying shades of red: How red team testing frameworks can enhance the cyber resilience of financial institutions. Financial Stability Institute. FSI Insights on Policy Implementation. 2019;(21). URL: https://www.bis.org/fsi/publ/insights21.pdf (дата обращения: 20.05.2020).
6. Конявский В.А., Ревенков П.В. Фролов Д.Б. и др. Кибербезопасность в условиях электронного банкинга: практическое пособие. М.: Прометей; 2020. 520 с.
7. Berdyugin A.A., Revenkov P.V. Approaches to measuring the risk of cyberattacks in remote banking services of Russia. *IT Security*. 2019;26(4):83–92. DOI: 10.26583/bit.2019.4.06
8. Скородумова О.Б., Скородумов Б.И., Матронина Л.Ф. Слагаемые качества обеспечения информационной безопасности. *Национальная безопасность / nota bene*. 2018;(2):1–9.
9. Васильева Е.В., Солянов К.С., Коневцева Т.Д. Адаптивное хранилище данных как технологический базис экосистемы банка. *Финансы: теория и практика*. 2020;24(3):132–146. DOI: 10.26794/2587–5671–2020–24–3–132–146
10. Фленов М.Е. Библия Delphi. СПб.: БХВ-Петербург; 2011. 688 с.
11. Козьминых С.И. Применение компьютерного имитационного моделирования для подготовки персонала на объектах топливно-энергетического комплекса. *Информационные ресурсы России*. 2019;3(169):2–8.
12. Lee L. Cybercrime has evolved: It's time cyber security did too. *Computer Fraud & Security*. 2019;2019(6):8–11. DOI: 10.1016/S 1361–3723(19)30063–6
13. Гисин В.Б., Славин Б.Б. и др. Парадигмы цифровой экономики: технологии искусственного интеллекта в финансах и финтехе. М.: Когито-Центр; 2019. 326 с.
14. Nikkel B. Fintech forensics: Criminal investigation and digital evidence in financial technologies. *Forensic Science International: Digital Investigation*. 2020;33:200908. DOI: 10.1016/j.fsidi.2020.200908
15. Крылов Г.О. Совершенствование процессов принятия решений при обработке больших данных в росфинмониторинге. *Современная математика и концепции инновационного математического образования*. 2020;7(1):143–152.

REFERENCES

1. King B. Bank 4.0: Banking everywhere, never at a Bank. Singapore: John Wiley & Sons Ltd; 2018. 352 p.
2. Skinner C. Digital human: The fourth revolution of humanity includes everyone. Singapore: Marshall Cavendish International (Asia) Pte Ltd; 2018. 400 p.
3. Revenkov P.V., Berdyugin A.A. Method of quantifying the risk of cyberattacks in the context of electronic banking. *Bankovskoye delo = Banking*. 2020;7:32–37. (In Russ.).
4. Salihu A., Metin H., Hajrizi E., Ahmeti M. The effect of security and ease of use on reducing the problems/deficiencies of Electronic Banking Services. *IFAC-PapersOnLine*. 2019;52(25):159–163. DOI: 10.1016/j.ifacol.2019.12.465

5. Kleijmeer R., Prenio J., Yong J. Varying shades of red: How red team testing frameworks can enhance the cyber resilience of financial institutions. Financial Stability Institute. FSI Insights on Policy Implementation. 2019;(21). URL: https://www.bis.org/fsi/publ/insights21.pdf (accessed on 20.05.2020).
6. Konyavskii V.A., Revenkov P.V., Frolov D.B. et al. Cybersecurity in the conditions of electronic banking: Practical guide. Moscow: Prometei; 2020. 520 p. (In Russ.).
7. Berdyugin A.A., Revenkov P.V. Approaches to measuring the risk of cyberattacks in remote banking services of Russia. *IT Security*. 2019;26(4):83–92. DOI: 10.26583/bit.2019.4.06
8. Skorodumova O.B., Skorodumov B.I., Matronina L.F. Components of the quality of information security. *Natsional'naya bezopasnost' / nota bene = National Security / nota bene*. 2018;(2):1–9. (In Russ.).
9. Vasilieva E.V., Solyanov K.S., Konevtseva T.D. Adaptive data warehouse as the technological basis of the banking ecosystem. *Finansy: teoriya i praktika = Finance: Theory and Practice*. 2019;24(3):132–146. (In Russ.). DOI: 10.26794/2587–5671–2019–24–3–132–146
10. Flenov M.E. The Delphi Bible. St. Petersburg: BHV-Petersburg; 2011. 688 p. (in Russ.).
11. Kozminykh S.I. The use of computer simulation for staff training at the facilities of fuel and energy complex. *Informatsionnye resursy Rossii = Information Resources of Russia*. 2019;(3):2–8. (In Russ.).
12. Lee L. Cybercrime has evolved: It's time cyber security did too. *Computer Fraud & Security*. 2019;2019(6):8–11. DOI: 10.1016/S 1361–3723(19)30063–6
13. Gisin V.B., Slavin B.B. et al. Paradigms of the digital economy: Artificial intelligence technologies in finance and fintech. Moscow: Cogito-Centre; 2019. 326 p. (In Russ.).
14. Nikkel B. Fintech forensics: Criminal investigation and digital evidence in financial technologies. *Forensic Science International: Digital Investigation*. 2020;33:200908. DOI: 10.1016/j.fsidi.2020.200908
15. Krylov G.O. Improving decision-making processes when processing big data in the Federal Financial Monitoring Service. *Modern mathematics and concepts of innovative mathematical education*. 2020;7(1):143–152.

ИНФОРМАЦИЯ ОБ АВТОРАХ / ABOUT THE AUTHORS

Александр Александрович Бердюгин — преподаватель Департамента информационной безопасности, Финансовый университет, Москва, Россия
Aleksandr A. Berdyugin — Lecturer, Department of Information Security, Financial University, Moscow, Russia
a40546b@gmail.com

Павел Владимирович Ревенков — доктор экономических наук, профессор Департамента информационной безопасности, Финансовый университет, Москва, Россия
Pavel V. Revenkov — Dr. Sci (Econ.), Prof., Department of Information Security, Financial University, Moscow, Russia
pavel.revenkov@mail.ru

Статья поступила в редакцию 28.06.2020; после рецензирования 24.08.2020; принята к публикации 12.09.2020. Авторы прочитали и одобрили окончательный вариант рукописи.
The article was submitted on 28.06.2020; revised on 24.08.2020 and accepted for publication on 12.09.2020. The authors read and approved the final version of the manuscript.