Владимир Д. Колычев[1], Николай А. Буданов[2]
Национальный исследовательский ядерный университет «МИФИ»
Каширское ш., 31, Москва, 115409, Россия
[1]e-mail: VDKolychev@mephi.ru, https://orcid.prg/0000-0002-8616-9354
[2]e-mail: NABudanov@mephi.ru, https://orcid.prg/0000-0002-9714-2915

КОМПЛЕКСНАЯ МЕТОДИКА ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОММЕРЧЕСКОМ БАНКЕ

DOI: http://dx.doi.org/10.26583/bit.2021.2.08

Аннотация. В данной статье рассматриваются методы увеличения защищенности информационной системы коммерческого банка. Предметом исследования является комплексная методика оценки информационной безопасности, используемая для определения уровня защищенности и риска информационной безопасности автоматизированной системы на основе прогнозных оценок и специализированного программного инструментария. Целью исследования и проводимого в работе анализа является повышение эффективности принимаемых решений при выполнении работ по оценке и управлению рисками в коммерческом банке. Результаты, представленные в рамках разработанной методики, могут быть использованы для решения задач увеличения надежности автоматизированной информационной системы в различных сферах и секторах деятельности, включая и организации промышленного сектора, а также коммерческие организации. Основные подходы, используемые при разработке комплексной методики оценки рисков, относятся к методам экспертного оценивания, теории случайных Марковских процессов, методам и моделям математической статистики и теории вероятностей, методам прикладного системного анализа и прогнозирования.

Ключевые слова: оценка рисков, информационные технологии, коммерческий банк, информационная система, средства защиты информации, автоматизированная информационная система.
Для цитирования: КОЛЫЧЕВ, Владимир Д.; БУДАНОВ, Николай А. КОМПЛЕКСНАЯ МЕТОДИКА ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОММЕРЧЕСКОМ БАНКЕ. Безопасность информационных технологий, [S.l.], v. 28, n. 2, p. 83–97, 2021. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1346>. Дата доступа: 29 apr. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.2.08.

Vladimir D. Kolychev[1], Nikolay A. Budanov[2]
National research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe shosse, 31, Moscow, 115409, Russia
[1]e-mail: VDKolychev@mephi.ru, https://orcid.prg/0000-0002-8616-9354
[2]e-mail: NABudanov@mephi.ru, https://orcid.prg/0000-0002-9714-2915

Development of a comprehensive methodology for assessing information security risks in a commercial bank

Abstract. This paper discusses the methods of improving the security of the information system of a commercial bank. The subject of the study is a comprehensive methodology for assessing information security used to determine the level of security and risk of information security of an automated system based on predictive estimates and specialized software tools. The purpose of the study and the carried out analysis are to improve the effectiveness of decisions made when performing work on risk assessment and management in a commercial bank. The results presented in the framework of the developed methodology can be used to solve the problems of increasing the reliability of an automated information system in various fields and sectors of activity, including organizations of the industrial sector, as well as commercial organizations. The main approaches used in the development of a comprehensive risk assessment methodology relate to the methods of expert assessment, the theory of random Markov processes, methods and models of mathematical statistics and probability theory, methods of applied system analysis and forecasting.

Keywords: risk assessment, information technology, commercial bank, information system, information security tools, automated information system.
For citation: KOLYCHEV, Vladimir D.; BUDANOV, Nikolay A. Development of a comprehensive methodology for assessing information security risks in a commercial bank. IT Security (Russia), [S.l.], v. 28, n. 2, p. 83– 2021. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1346>. Date accessed: 29 apr. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.2.08.

Введение

Задачи исследования информационной безопасности (ИБ) в сфере корпоративных банковских информационных систем остаются по-прежнему актуальными, особенно в связи с ростом объема обрабатываемых массивов данных, повышения требований к надежности и отказоустойчивости программно-аппаратных комплексов технических средств [1].

Используемая система защиты корпоративных информационных систем на предприятии включает в качестве составных компонентов технические и программно-аппаратные средства защиты, организационно-методическое обеспечение, а также подсистемы гарантирующие надежность и высокую степень безопасности обрабатываемых данных.

Например, в [1] «предметом исследования является комплексная оценка системы информационной безопасности, предоставляющая возможность определения уровня защищенности информационной системы на основе прогнозных оценок. Объектом исследования является набор методов, обеспечивающих информационную безопасность корпоративных информационных систем, а также методика анализа рисков».

В отличие от [1], в данной статье дается описание разработки комплексной методики оценки и управления рисками информационной безопасности коммерческого банка на основе прогнозирования инцидентов информационной безопасности, вызванных субъективными и объективными дестабилизирующими факторами.

1. Разработка моделей бизнес-процессов комплексной оценки рисков в коммерческом банке

Динамика внедрения проектов развития информационных систем в банковской сфере и сокращение числа коммерческих банков свидетельствует о необходимости повышения требования к защищённости информационных системы, повышению надежности и отказоустойчивости их функционирования, обеспечения целостности, доступности, конфиденциальности и качества обработки информации. На рис. 1 представлена динамика изменения количества коммерческих банков [2], причем тенденция к сокращению их числа будет сохраняться и в дальнейшем[1].

Таким образом, наиболее финансово устойчивые коммерческие структуры в банковском секторе обладают высокотехнологичными информационными системами и сервисами, построенными на принципах комплексной защиты информации и предотвращения утечек персональных данных клиентов в связи с участившимися в последнее время фактами мошенничества.

[1]Количество банков в России по годам. URL: http://fincan.ru/articles/53_kolichestvo-bankov-v-rossii-po-godam/#:~:text=Динамика%20количества%20банков%20в%20России.,2018%20г.%20–%20уже%2057 (дата обращения: 14.04.2021)

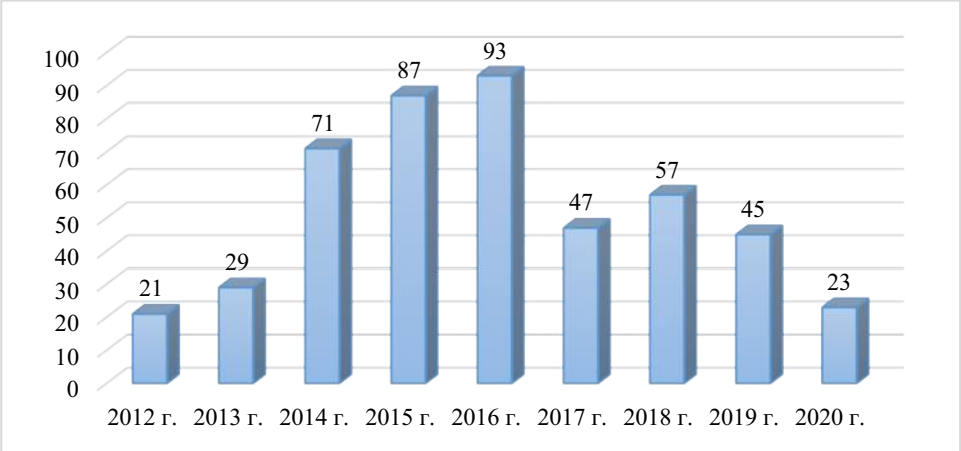

Рис. 1. Динамика отзыва лицензий у коммерческих банков на территории РФ [2]
Fig. 1. Dynamics of revocation of licenses from commercial banks in the Russian Federation [2]

В настоящее время в связи с использованием процессного подхода разрабатываются требования к формированию системы информационной безопасности коммерческого банка, которая определяется как состояние безопасности целей предприятия в условиях угроз для информационной среды [3].

Работы по обеспечению информационной безопасности коммерческого банка, в силу определенной специфики, оказывают непосредственное влияние на функционирование организации посредством:

- документации, регламентирующей информационную безопасность, в том числе и аффилированных структурных подразделений;
- методов контроля информационной безопасности, основываясь на статистических данных об инцидентах и угрозах, данных мониторинга информационной и аудита безопасности информационной системы;
- комплексного характера интересов и целей бизнес-деятельности предприятия в области информационного контроля, с учетом деятельности структурных подразделений предприятия [4].

Разработанная авторами схема оценки рисков информационной безопасности на предприятии представлена на рис. 2. В разработанной модели бизнес-процесса представлен подход к обеспечению безопасности информационной системы, включая следующие основные элементы: идентификация угроз, общее описание анализа мер обеспечения безопасности, позволяющее проводить детализированное исследование в рамках конкретной информационной системы. При этом необходимо определение комплекса защитных мер (технических, организационных, административных или технологических) для противостояния внешним угрозам [5, 6].

Следует при этом отметить, что деятельность в области анализа информационной безопасности представлена следующими этапами: идентификация и оценка характеристик угроз информационной безопасности, оценка защищенности компонентов, оценка ценности привлекаемых и используемых инфраструктурных ресурсов, документирование результатов, включая комплекс разработанных мероприятий по обеспечению информационной безопасности [6].

2. Обзор нормативно-методического инструментария оценки рисков в коммерческом банке

В основу комплексной методики заложены методы прикладного системного анализа информационной безопасности коммерческого банка, включающие применение интегрированных средств защиты информации.

В качестве нормативно-методического инструментария при разработке комплексной методики оценки рисков использован ряд отечественных[2] и зарубежных стандартов в сфере информационной безопасности: Международный стандарт ISO/IEC 1779-2005, стандарт Cobit 4 Edition (США), NIST 800-30, стандарт BS ISO 27002:2005 (Великобритания).

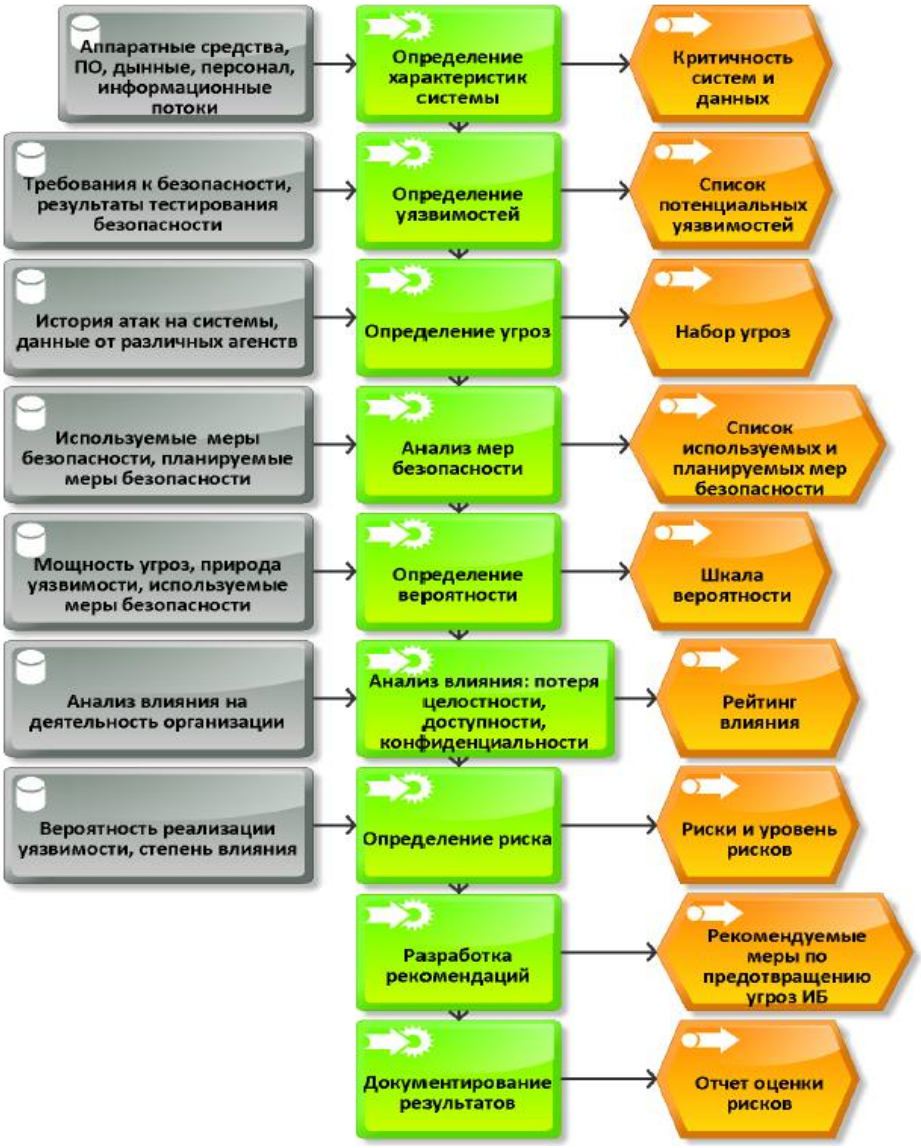

Рис. 2. Схема оценки рисков информационной безопасности
Fig. 2. Information security risk assessment scheme

[2]ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» ГОСТ Р ИСО/МЭК 31010-2011 «Менеджмент риска. Методы оценки риска»

Согласно действующим российским и международным нормативным документам идентификация угроз информационной безопасности проводится на основе сформированного перечня угроз, принимая во внимание частоту их возникновения, используя для исследования и анализа формат реестра или базы данных. Среди факторов, оказывающих существенное влияние на процесс анализа рисков информационной безопасности, следует выделить: наличие и доступность ресурсов коммерческого банка, кадровый состав, информационную инфраструктуру, нормативно-методическое обеспечение и рабочую документацию, аппаратные средства и программное обеспечение, оборудование для обеспечения связи.

Результатом оценивания рисков является список оцененных рисковых ситуаций по каждому отдельному инциденту информационной безопасности, включая также дополнительные факторы, связанные с разграничением прав доступа, модификацией и разрушением информационной инфраструктуры коммерческого банка (нарушением функционирования сервисов и подсистем) [7, 8].

Разработанная с учетом действующих стандартов схема деятельности по обеспечению информационной безопасности и оценке рисков представлена на рис. 3.

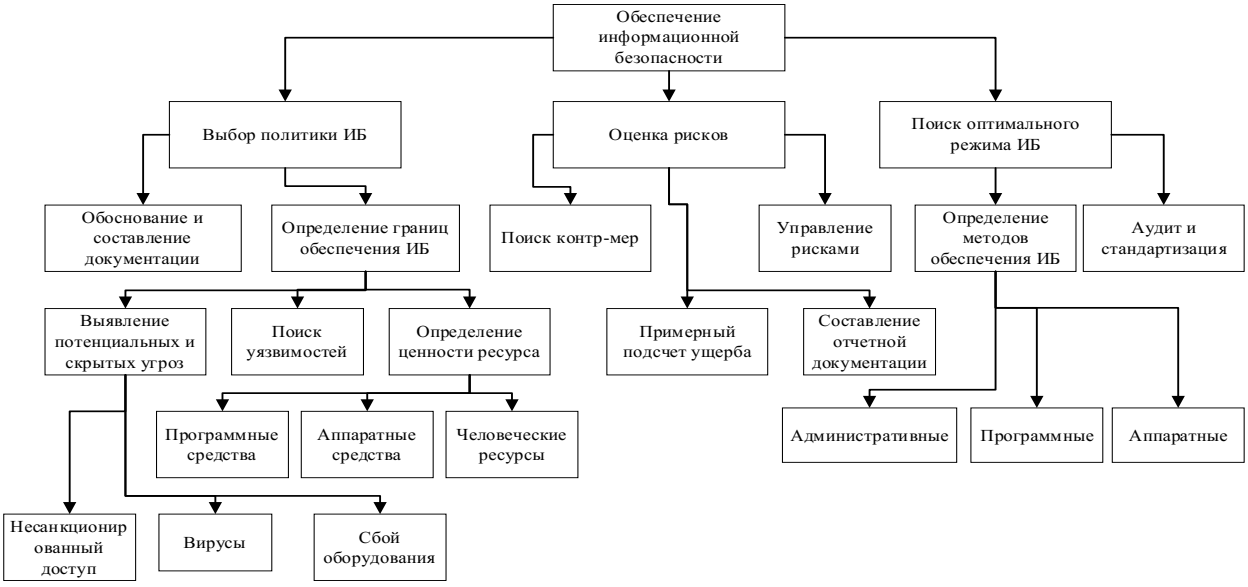

Рис. 3. Схема деятельности по обеспечению информационной безопасности и оценке рисков
Fig. 3. Outline of information security and risk assessment activities

Большинство методик[3] и стандартов[4] оценки информационной безопасности выстраивается на основе моделирования состава объектов, обобщённая модель структуры комплекса программно-технических средств, представлена на рис. 4.

Автоматизированная информационная система (АИС) коммерческого банка включает следующие компоненты:

- Сервер обработки, с помощью которого обрабатываются данные;
- Маршрутизатор для объединения внутренней сети Intranet с внешней Internet;

[3]Методический документ «Методика оценки угроз безопасности информации» (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.)
[4]Стандарт Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации/ Общие положения» (принят и введен в действие распоряжением Банка России от 17 мая 2014 г. № Р-399)

- Сервер БД, выполняющий обслуживание и управление базой данных и отвечает за целостность и сохранность данных, а также обеспечивает операции ввода-вывода при доступе клиента к информации;

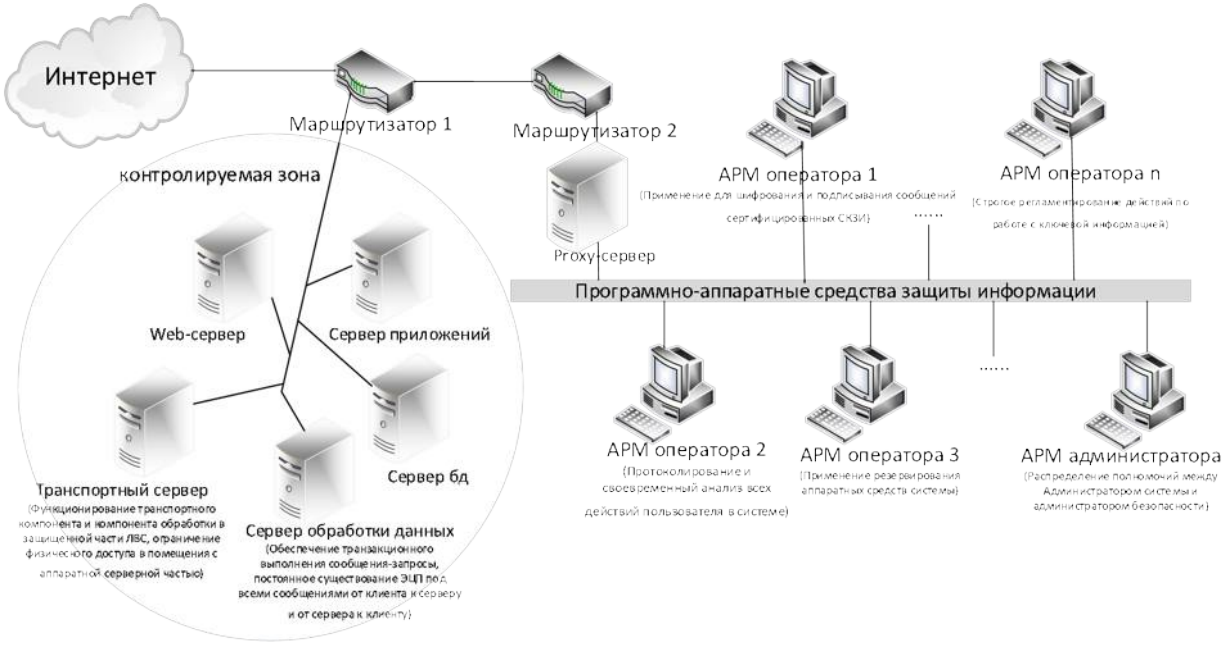

Рис. 4. Обобщенная структура комплекса программно-технических средств информационной системы

Fig. 4. Generalized structure of the complex of software and hardware tools of the information system

- Транспортный сервер, осуществляющий перенаправление информационных потоков;
- Proxy-сервер, осуществляющий мониторинг действий пользователей вне локальной сети;
- Сервер приложений, предназначенный для эффективного исполнения процедур (программ, скриптов), на которых построены приложения, а также для идентификации пользователей посредством разработанных приложений;
- Веб-сервер, предназначенный для получения доступа к внутренним информационным ресурсам организации;
- Администраторский АРМ для управления системой;
- Множество АРМ пользователей – операторов.

3. Разработка методики и реализация алгоритмов оценки рисков информационной безопасности в коммерческом банке

На основе принципов [9, 10] и стандартов информационной безопасности, разработана комплексная методика оценки рисков информационной безопасности в коммерческом банке, состоящая из следующих этапов: описание характеристик информационной системы (включая выделенные компоненты), формирование моделей нарушителя и угроз, ранжирование и оценивание важных угроз (с использованием методов экспертной оценки), оценка и прогнозирование инцидентов в соответствии с субъективными дестабилизирующими факторами (с использованием экспертных методов), оценка инцидентов в соответствии с субъективными дестабилизирующими факторами (с использованием экспертных методов), формирование отчетов,

направленных на принятие мер по совершенствованию или построению системы по защите информации [11].

На стадии описания характеристик информационной системы определяется множество объектов информационной системы (ИС), которые формально представляются в вид $s_i \in \{S\}$, где S – общее количество компонентов информационной системы, $i \in 1 \ldots n$, а n – общее количество компонентов информационной безопасности. На основе разработанных моделей по обеспечению информационной безопасности и оценке угроз были разработаны компоненты модели объекта, на который направлены угрозы. Модель объекта включает следующие атрибуты: инфраструктура, различные виды коммуникационных информационных сетей, компоненты систем передачи данных, база данных, стандартное ПО и др.

В свою очередь, модель угроз для информационной системы включает две выделенные категории угроз: объективные и субъективные, которые в свою очередь подразделяются на внешние и внутренние угрозы.

Для информационной системы коммерческого банка модель нарушителя основывается на трех категориях нарушителей в соответствии с правами доступа в контролируемую зону: внешние (хакеры), внутренние (партнеры) и внутренние (персонал). Внутренние нарушители разделяются на уровни согласно правам доступа в интегрированную АИС предприятия, также выделяют внешних нарушителей согласно их уровню осведомленности о параметрах информационной системы – клиенты, партнеры, контрагенты, поставщики и др.

Важными компонентами модели нарушителя являются общедоступное и специализированное программное обеспечение, включая программные компоненты, разработанные злоумышленниками, находящиеся в сети интернет в свободном доступе, использующие известные уязвимости («черви», вирусы, exploit, сканеры безопасности и др.). Как правило, злоумышленникам становится доступной следующая информация об объекте атаки: юридический и нормативно-правовой статус, сфера деятельности и технологии безопасности, сведения о топологических характеристиках корпоративной вычислительной сети, сведения о доступных для атаки портах рабочих станций и на сервере, используемое ПО, идентификационные пользовательские данные, методы защиты конфиденциальной информации и др.

Для оценки числа инцидентов, ранжирования и оценивания важных угроз информационной безопасности в АИС используются методы экспертной оценки [11, 12] в соответствии со следующим алгоритмом:

1. Формируется множество (пул) экспертов из числа компетентных специалистов в области информационной безопасности и сфере ИТ, создается анкета для оценивания уровня компетентности и вероятностей реализации угрозы, возможности восстановления системы после возникновения угрозы;
2. Оценивается профессионализм каждого эксперта (специалиста);
3. Эксперт заполняет предложенную анкету, в которой следует отметить количество инцидентов, которые, могут произойти на протяжении одного периода (как правило, месяца) в автоматизированной банковской информационной системе;
4. Проводится оценка согласованности мнения экспертов в соответствии с дисперсионным коэффициентом конкордации W и оценивается уровень значительности коэффициента, согласно критерию Пирсона χ^2;
5. Определяется результирующее (итоговое) значение инцидентов в сфере ИБ $r_i = \frac{\sum_{j=1}^{m} r_{ij}}{K_j}$, учитывая коэффициент компетентности каждого эксперта, где параметр

r_{ij} – оценка, принадлежащая *j*-му эксперту *i*-му фактору, $i \in 1..n$, $j \in 1..m$, (*n* – общее число экспертов, а *m* – число факторов), *K* – расчетный параметр компетентности *j* – го эксперта, т.е. его компетентность.

Определение степени компетентности экспертов реализуется на основе следующего алгоритмического подхода:

1. Специалист (компетентный эксперт) заполняет анкету, отвечая на предложенные вопросы;

2. Ответы на анкетные вопросы со стороны эксперта сохраняются в БД, проводится расчет, и получают коэффициент компетентности каждого опрошенного эксперта K_i;

3. Рассчитанные показатели нормируются $K_j = \frac{K_j}{\sum_j^1 K_j}$ и затем используются при расчете количества инцидентов информационной безопасности.

С целью определения числовой оценки согласованности экспертов, используется коэффициент конкордации *W*, рассчитываемый на основе следующего соотношения: $W = \frac{12S}{m^2(n^3-n)-m\sum_{j=1}^{m} T_j}$, где *S* – сумма квадратов отклонений, $S = \sum_{i=1}^{n}\left(\sum_{j=1}^{m} r_{ij} - \bar{r}\right)^2$, $\bar{r} = \frac{1}{n}\sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij}$, T_j – индикатор связанных рангов при ранжировании *j*-го эксперта, $T_j = \sum_{K=1}^{H_j} h_k^3 - h_k$, где h_k – количество совпадающих рангов в *k*-й группе связанных рангов; H_j – количество групп совпадающих рангов в ранжировании *j*-го эксперта.

Коэффициент конкордации *W* численно изменяется в диапазоне $0 \le W \le 1$. Верхняя граница обозначает, одинаковые оценки информативности факторов, которые проставили эксперты, нижняя граница отображает отсутствие связи между оценками, которые получены от разных экспертов [12, 13].

Оценка значимости коэффициента конкордации *W* выполняется в соответствии с критерием Пирсона χ^2 с применением соотношения: $\chi^2 = \frac{12S}{mn(n+1)-\frac{1}{n-1}\sum_{j=1}^{m} T_j}$.

Вычисленное значение критерия χ^2 сопоставляется с пороговым значением $\chi^2_{кр}(a, n-1)$ по степени значимости α, а также и по количеству степеней свободы *n* − 1. В том случае, если выполняется соотношение $\chi^2 \ge \chi^2_{кр}$, экспертные оценки считаются согласованными. Вероятность осуществления угроз информационной безопасности для автоматизированной системы определяется на основе соотношения: $P(t) = 1 - e^{-\lambda t}$, где λ – интенсивность осуществления угрозы ИБ, *t* − общее количество времени функционирования банковской информационной системы.

Для выделенных экспертами угроз информационной безопасности вычисляется значение P_{X_j} по расчетным вероятностям согласно шкалам оценки вероятностей.

Оценивание степени воздействия угроз информационной безопасности в коммерческом банке реализуется посредством следующего подхода:

1. Администратор безопасности знакомится с предлагаемой шкалой оценки степени воздействия угроз информационной безопасности в коммерческом банке;

2. Администратор безопасности заполняет предлагаемую анкету по оценке степени воздействия L_{X_j} любой угрозы на информационную систему коммерческого банка.

Оценивается вероятность восстановления по окончанию выполнения угроз ИБ посредством следующего алгоритма:

1. Экспертам представляется для ознакомления шкала оценки вероятности возобновления АИС;

2. Экспертам предлагается оценить вероятность возобновления работоспособности АИС после реализации набора реализованных угроз информационной безопасности;

3. Оценивается согласованность специалистов в соответствии с дисперсионным коэффициентом конкордации *W*, а также оценивается уровень значимости расчетного коэффициента, согласно критерию Пирсона χ^2.

4. Определяется результирующее значение вероятности возобновления функционирования АИС после реализации набора угроз, учитывая коэффициент компетентности каждого специалиста. При этом оценка значимости угроз ИБ, считается необходимой, с целью идентификации угроз ИБ, которые являются наиболее опасными.

В качестве результирующих данных используют вероятность осуществления угроз P_{X_j}, с множеством допустимых значений *P* = [0,1] и множеством базовых значений *Tp* = {очень высокая, высокая, средняя, низкая, очень низкая}= $\{a_{X_1}, a_{X_2}, a_{X_3}, a_{X_4}, a_{X_5}\}$ и уровнем воздействия угроз ИБ L_{X_j} с областью допустимых значений *L* = [0,1] и множеством базовых значений T_L = {разрушительное воздействие, критическое воздействие, тяжелое воздействие, умеренное воздействие, легкое воздействие}[1].

Уровень значимости угрозы ИБ F_{X_j} с областью допустимых значений *F* = [0,1] и множеством базовых значений T_F = {разрушительное, большое, среднее, малое, несущественное} = $\{a_{V_1}, a_{V_2}, a_{V_3}, a_{V_4}, a_{V_5}\}$, считается выходным параметром модели.

Таким образом, на основе существующих методов оценивания и предлагаемых алгоритмов оценки определяется:

- множество значительных угроз, которые способен осуществить нарушитель в ИС $x_{ij} \in \{X\}$, где $i \in 1 \dots kj \in 1 \dots m$, *m* – общее количество угроз ИБ, *k* – общее количество нарушителей ИБ;
- множество важных угроз ИБ для любого из объектов $x_{js_i} \in \{X\}$ и для любого из нарушителей $x_{i,js_i} \in \{X\}$;
- множество важных угроз ИБ для любого объекта и для любого нарушителя, которые относятся к классам: конфиденциальности $\{K\} - k_{js_i}, k_{i,js_i} \in \{K\} \subset \{X\}$; целостности $\{C\} - c_{js_i}, c_{i,js_i} \in \{C\} \subset \{X\}$; доступности $\{D\} - d_{js_i}, d_{i,js_i} \in \{D\} \subset \{X\}$.

После оценки уровня воздействия угроз ИБ, значения значимых угроз нормируются для: всех важных угроз ИБ $P_{норм}(x_j) = \frac{P(x_j)}{\sum_{j=1}^{m} P(x_j)}$; любого объекта ИС $P_{норм}(x_{js_i}) = \frac{P(x_{js_i})}{\sum_{j=1}^{m} P(x_{js_i})}$; любого объекта ИС по доступности, целостности и конфиденциальности $P_{норм}(k_{js_i}) = \frac{P(k_{js_i})}{\sum_{j=1}^{m} P(k_{js_i})}$; $P_{норм}(c_{js_i}) = \frac{P(c_{js_i})}{\sum_{j=1}^{m} P(c_{js_i})}$. Аналогичным образом нормируют вероятности неполного или частичного возобновления функций.

Далее определяется абсолютная вероятность осуществления угроз ИБ для любого объекта, нарушителя и абсолютная вероятность осуществления угроз для любого объекта ИС по трем категориям угроз: доступности, целостности и конфиденциальности [1]. Разработанная схема модели оценки рисков информационной безопасности в коммерческом банке представлена на рис. 5. Основное задачей создания методики оценки информационной безопасности является оценивание возможности использования выходных данных модели, с целью их применения в качестве входных для разработки рекомендаций для увеличения степени безопасности в автоматизированной ИС коммерческого банка.

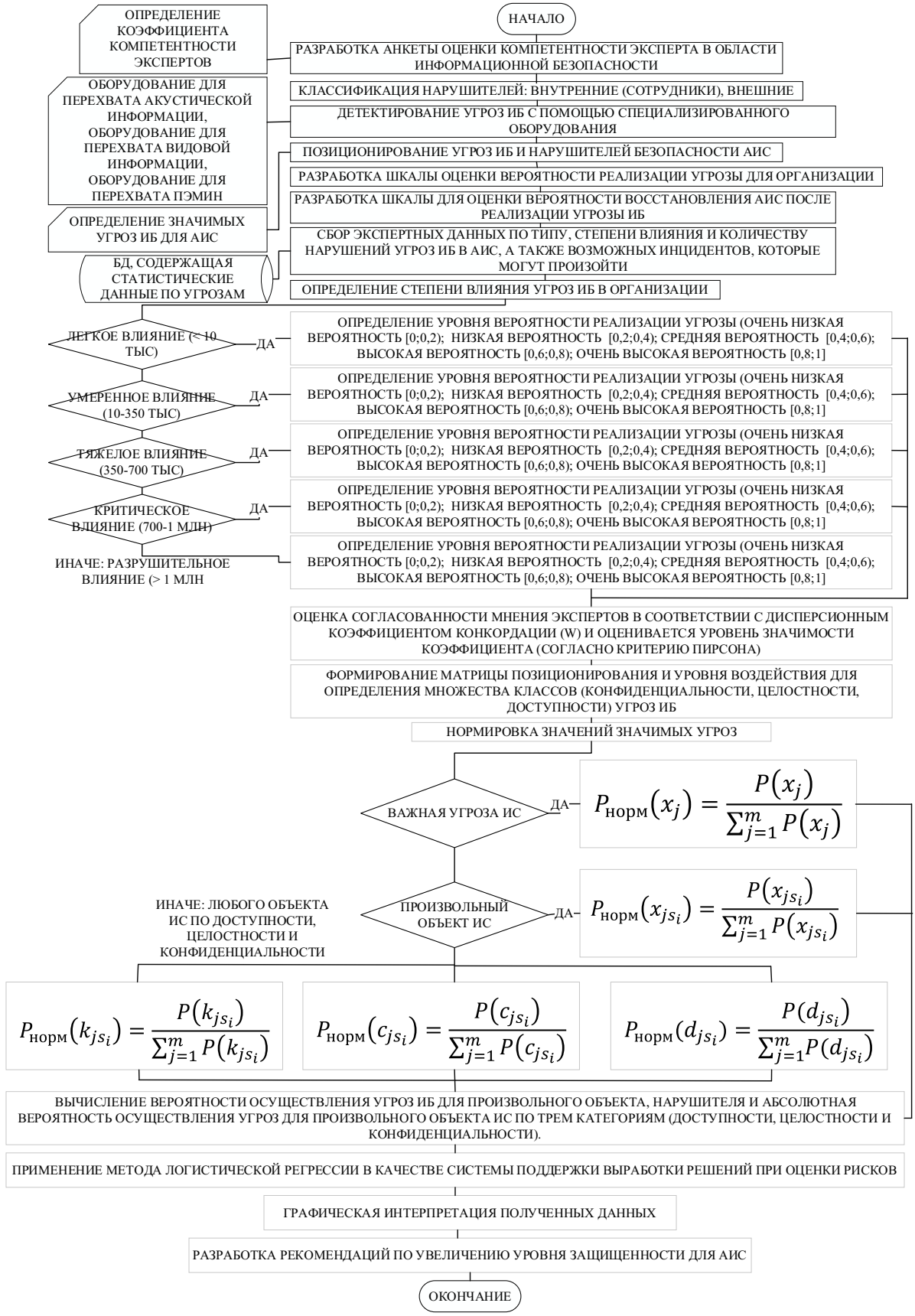

Рис. 5. Схема модели оценки рисков информационной безопасности в коммерческом банке
Fig. 5. Diagram of the information security risk assessment model in a commercial bank

С целью оценивания количества случаев нарушения ИБ коммерческого банка, была сформирована группа экспертов, проведена проверка согласованности их мнения, осуществлен сбор экспертных данных по типу, степени влияния угроз ИБ в АИС на основе разработанных шкал оценки, полученные результаты были занесены в разработанную базу данных, выполнено вычисление вероятности осуществления угроз ИБ, использованием метода логистической регрессии реализована проверка качества данных.

На рис. 6–11 представлены рассчитанные с использованием разработанной модели вероятности реализации и восстановления после реализации выделенного набора угроз информационной безопасности для компонент АИС коммерческого банка.

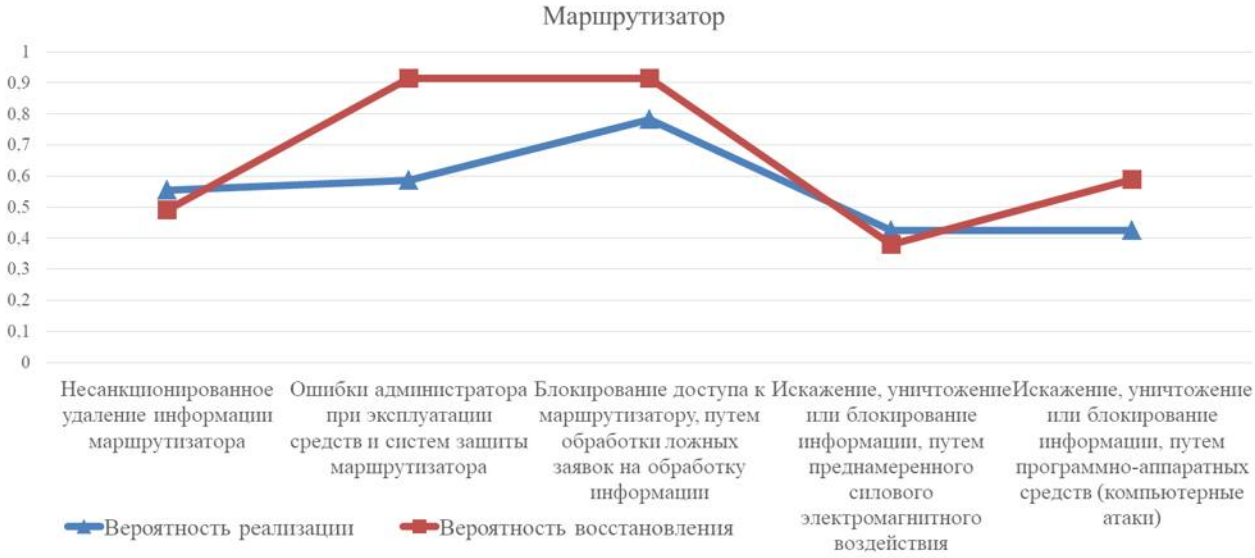

Рис. 6. Вероятности реализации и восстановления после реализации набора угроз для маршрутизатора

Fig. 6. Probabilities of implementation and recovery after a threat set to the router

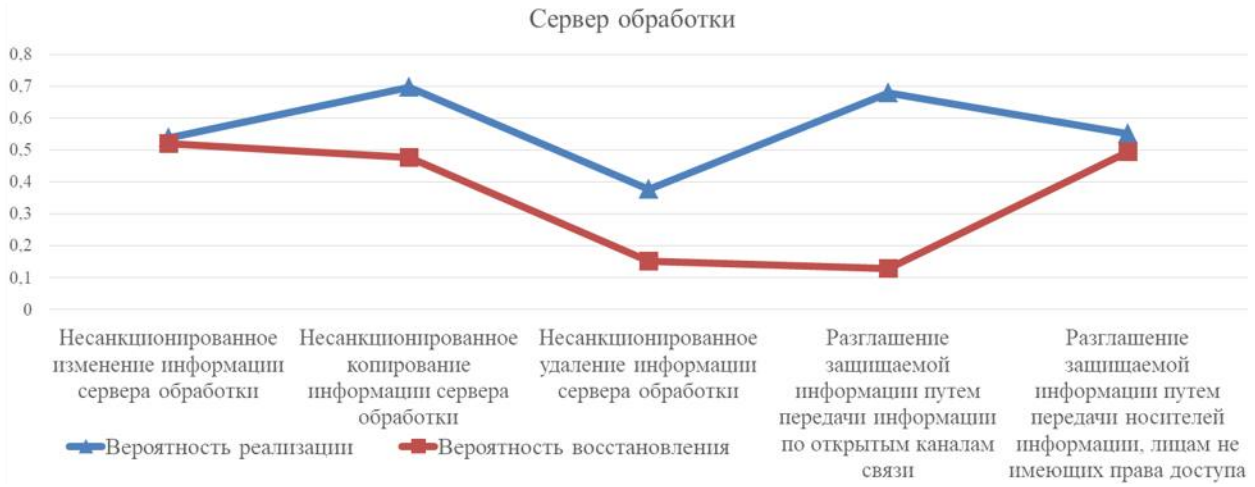

Рис. 7. Вероятности реализации и восстановления после реализации набора угроз для сервера обработки

Fig. 7. Probabilities of implementation and recovery after a threat set to the processing server

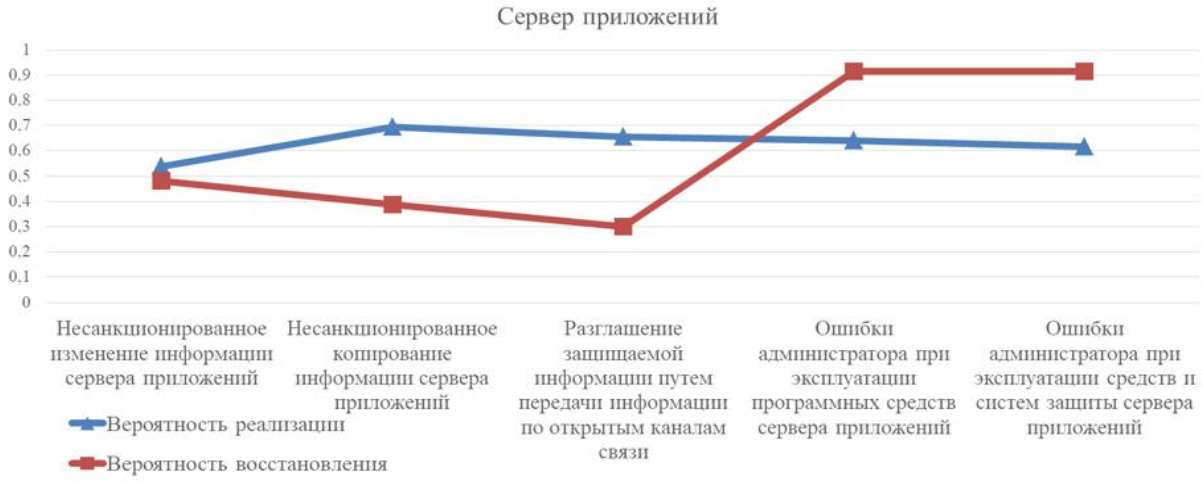

Рис. 8. Вероятности реализации и восстановления после реализации набора угроз для сервера приложений

Fig. 8. Probabilities of implementation and recovery after a threat set to the application server

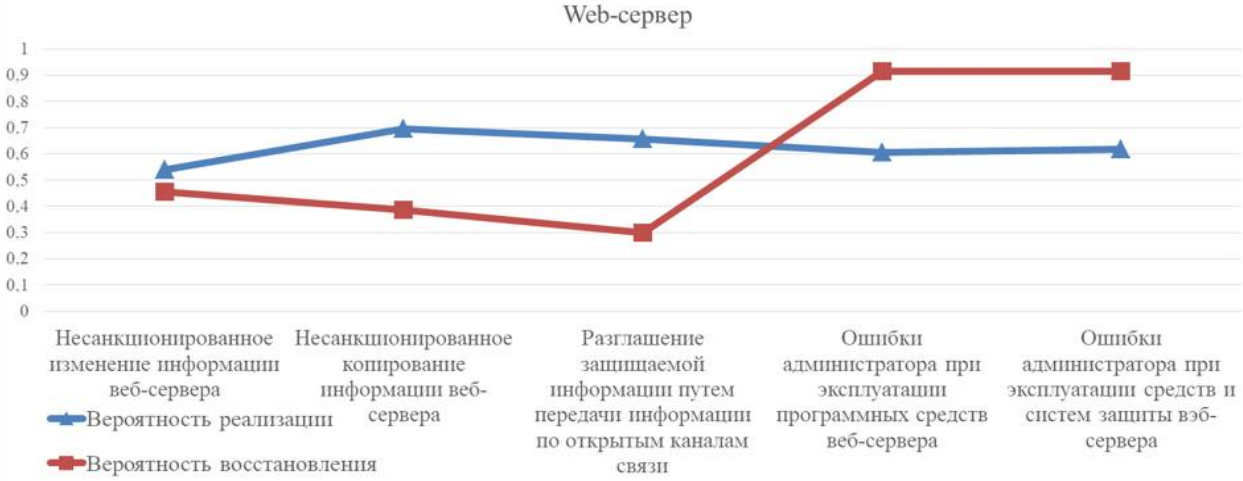

Рис. 9. Вероятности реализации и восстановления после реализации набора угроз для веб-сервера

Fig. 9. Probabilities of implementation and recovery after a threat set to the web server

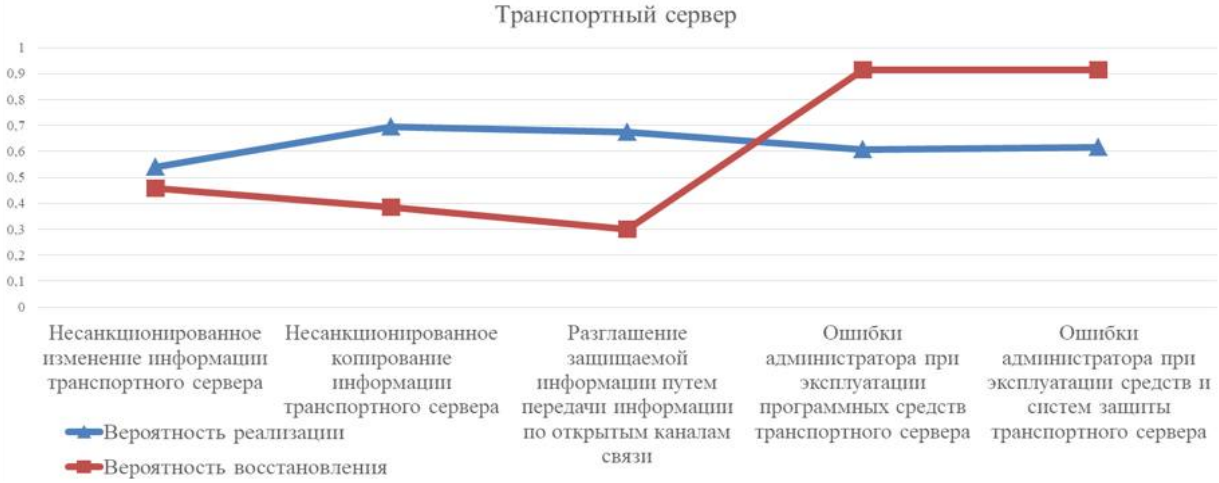

Рис. 10. Вероятности реализации и восстановления после реализации набора угроз для транспортного сервера

Fig. 10. Probabilities of implementation and recovery after a threat set to the transport server

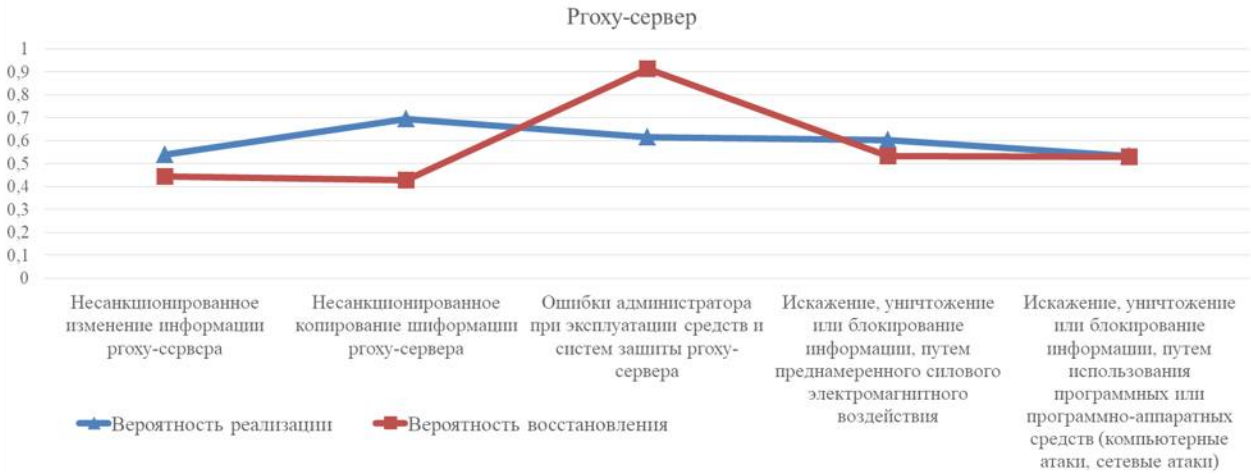

Рис. 11. Вероятности реализации и восстановления реализации набора угроз для Proxy-сервера
Fig. 11. Probabilities of implementation and recovery after a threat set to the Proxy server

Заключение

Решение задач повышения надежности средств защиты информации автоматизированной информационной системы коммерческого банка является комплексной проблемой, требующей своевременного и оперативного решения особенно в условиях увеличивающегося объема обрабатываемой информации и возрастающего количества атак злоумышленников на кредитные организации.

В данной статье выполнен анализ действующих стандартов в сфере информационной безопасности. Результаты проведенного анализа показывают, что большая часть стандартов регламентируют требования безопасности, не включая количественного подхода к оценке рисков. Выполнено моделирование бизнес-процессов комплексной оценки рисков в организации, разработана схема деятельности по обеспечению информационной безопасности и оценке рисков. Разработана архитектура системы информационной безопасности коммерческого банка с учетом структуры комплекса программно-технических средств.

С использованием методов экспертных оценок, статистического анализа данных, инструментальных средств создания баз данных разработана комплексная методика оценки рисков информационной безопасности в коммерческом банке. Разработан алгоритм вычисления вероятностей восстановления информационной системы после реализации набора угроз информационной безопасности, принимая во внимание факторы и уровни значимости и важности реализации угроз с учетом технических и эксплуатационных характеристик компонентов автоматизированной информационной системы.

Результаты тестирования комплексной модели оценки рисков информационной безопасности свидетельствуют об устойчивости получаемых значений вероятностей с точки зрения надежности функционирования информационной инфраструктуры коммерческого банка. Полученные вероятности позволят скорректировать политики информационной безопасности и повысить защищенность информационной системы за счет принятия системы мер, направленных на совершенствование комплекса программно-технических средств, а также информационных сервисов предприятия.

Предлагаемая методика может быть использована для оценки рисков информационной безопасности на предприятиях и в организациях различных сфер деятельности, ориентированных на финансово-банковский сектор.

СПИСОК ЛИТЕРАТУРЫ:

1. Ерохин С.С. Методика аудита информационной безопасности объектов электронной коммерции. Автореферат диссертации на соискание ученой степени кандидата технических наук. Томск. 2010. URL: https://www.elibrary.ru/item.asp?id=19323991 (дата обращения: 14.04.2021).
2. Балашев Н.Б., Ушаков А.И. Динамика формирования кредитной системы РФ // Научно-методический электронный журнал «Концепт». 2020. № 04 (апрель). С. 113–124. URL: http://e-koncept.ru/2020/203007.htm. DOI: https://doi.org/10.24411/2304-120X-2020-13007 (дата обращения: 14.04.2021).
3. Leonova N.M., Modyaev A.D., Kolychev V.D. Visualization of a product's life cycles in the common information space on the basis of project management methods. Scientific Visualization, 2016, 8(5). С. 26–40. URL: http://sv-journal.org/2016-5/03/en/index.php?lang=ru (дата обращения: 14.04.2021).
4. Kulik S.D. Model for evaluating the effectiveness of search operations. Journal of ICT Research and Applications. Vol. 9, Issue 2, 2015. P. 177–196. DOI: https://doi.org/10.5614/itbj.ict.res.appl.2015.9.2.5.
5. Miloslavskaya N., Furnell S. (2021) Network Security Intelligence Centres for Information Security Incident Management. In: Samsonovich A.V., Gudwin R.R., Simões A.S. (eds) Brain-Inspired Cognitive Architectures for Artificial Intelligence: BICA*AI 2020. BICA 2020. Advances in Intelligent Systems and Computing, vol 1310. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-65596-9_34.
6. Miloslavskaya N., Tolstaya S. (2020) On the Assessment of Compliance with the Requirements of Regulatory Documents to Ensure Information Security. In: Rocha Á., Adeli H., Reis L., Costanzo S., Orovic I., Moreira F. (eds) Trends and Innovations in Information Systems and Technologies. WorldCIST 2020. Advances in Intelligent Systems and Computing, vol 1160. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-45691-7_74.
7. Нестерова Д.А. Риски информационной безопасности коммерческих банков в условиях новой экономической и технологической реальности. Инновации и инвестиции, 2020, № 5. С. 144–150. URL: https://www.elibrary.ru/item.asp?id=43066036 (дата обращения: 14.04.2021).
8. Бердюгин А.А. Управление риском нарушения информационной безопасности в условиях электронного банкинга. Вопросы кибербезопасности №1(25), 2018. С. 28–38. DOI: https://doi.org/10.21681/2311-3456-2018-1-28-38.
9. Melnikov D.A., Durakovsky A.P., Dvoryankin S.V. and Gorbatov V.S. Concept for Increasing Security of National Information Technology Infrastructure and Private Clouds. 2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud), Prague, 2017. P. 155–160. DOI: https://doi.org/10.1109/FiCloud.2017.11.
10. Korsakov I.A., Durakovskiy A.P. (2020) About the Security Assessment of Embedded Software in Automated Process Control System. In: Misyurin S., Arakelian V., Avetisyan A. (eds) Advanced Technologies in Robotics and Intelligent Systems. Mechanisms and Machine Science, vol 80. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-33491-8_46.
11. Будзко В.И., Ядринцев В.В., Соченков И.В., Королёв В.И., Беленков В.Г. Формирование в системах интенсивного использования данных маркеров конфиденциальности в условиях высокой неопределенности при их использовании. В сборнике: Информационные технологии и математическое моделирование систем 2020. Труды международной научно-технической конференции. 2020. С. 81–89. DOI: https://doi.org/10.36581/CITP.2020.11.36.020.
12. Keyun Ruan. Introducing cybernomics: A unifying economic framework for measuring cyber risk. Computers & Security, 2017, vol. 65. P. 77–89. DOI: https://doi.org/10.1016/j.cose.2016.10.009.
13. Попов Г.А., Попов А.Г. Результирующая оценка при наличии нескольких вариантов оценивания на примере задач информационной безопасности. Вестник астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2017. № 1. С. 48–61. URL: https://www.elibrary.ru/item.asp?id=28147036 (дата обращения: 14.04.2021).

REFERENCES:

[1] Erokhin S.S. Methodology of audit of information security of electronic commerce objects. Abstract of the dissertation for the degree of Candidate of Technical Sciences. Tomsk. 2010. URL: https://www.elibrary.ru/item.asp?id=19323991 (accessed: 14.04.2021) (in Russian).
[2] Balashev N.B., Ushakov A.I. Dynamics of the credit system formation in the Russian Federation. Saentific and methodological electronic journal “Koncept”, 2020. No. 04. P. 113–124. URL: http://e-koncept.ru/2020/203007.htm. DOI: https://doi.org/10.24411/2304-120X-2020-13007 (accessed: 14.04.2021) (in Russian).

[3] Leonova N.M., Modyaev A.D., Kolychev V.D. Visualization of a product's life cycles in the common information space on the basis of project management methods. Scientific Visualization, 2016, 8(5). P. 26–40. (in Russian).
[4] Kulik S.D. Model for evaluating the effectiveness of search operations. Journal of ICT Research and Applications. Vol. 9, Issue 2, 2015. P. 177–196. DOI: https://doi.org/10.5614/itbj.ict.res.appl.2015.9.2.5.
[5] Miloslavskaya N., Furnell S. (2021) Network Security Intelligence Centres for Information Security Incident Management. In: Samsonovich A.V., Gudwin R.R., Simões A.S. (eds) Brain-Inspired Cognitive Architectures for Artificial Intelligence: BICA*AI 2020. BICA 2020. Advances in Intelligent Systems and Computing, vol 1310. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-65596-9_34.
[6] Miloslavskaya N., Tolstaya S. (2020) On the Assessment of Compliance with the Requirements of Regulatory Documents to Ensure Information Security. In: Rocha Á., Adeli H., Reis L., Costanzo S., Orovic I., Moreira F. (eds) Trends and Innovations in Information Systems and Technologies. WorldCIST 2020. Advances in Intelligent Systems and Computing, vol 1160. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-45691-7_74.
[7] Nesterova D.A. Risks of information security of commercial banks in the new economic and technological reality. Innovation and investment, 2020, no. 5, P. 144–150. URL: https://www.elibrary.ru/item.asp?id=43066036 (accessed: 14.04.2021) (in Russian).
[8] Berdyugin A.A. Risk management of information security violation in conditions of electronic banking. Voprosy Kiberbezopasnosti, No 1(25) – 2018. P. 28-38. DOI: https://doi.org/10.21681/2311-3456-2018-1-28-38 (in Russian).
[9] Melnikov D.A., Durakovsky A.P., Dvoryankin S.V. and Gorbatov V.S. Concept for Increasing Security of National Information Technology Infrastructure and Private Clouds 2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud), Prague, 2017. P. 155–160. DOI: https://doi.org/10.1109/FiCloud.2017.11.
[10] Korsakov I.A., Durakovskiy A.P. (2020) About the Security Assessment of Embedded Software in Automated Process Control System. In: Misyurin S., Arakelian V., Avetisyan A. (eds) Advanced Technologies in Robotics and Intelligent Systems. Mechanisms and Machine Science, vol 80. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-33491-8_46.
[11] Budzko V.I., Yadrentsev V.V., Sochenkov I.V., Korolev V.I., Belenkov V.G. Formation of privacy markers in systems of intensive use of data under conditions of high uncertainty when using them. In the collection: Information Technologies and mathematical modeling of systems 2020. Proceedings of the International Scientific and Technical Conference. 2020. P. 81–89. DOI: https://doi.org/10.36581/CITP.2020.11.36.020 (in Russian).
[12] Keyun Ruan. Introducing cybernomics: A unifying economic framework for measuring cyber risk. Computers & Security, 2017, vol. 65. P. 77–89. DOI: https://doi.org/10.1016/j.cose.2016.10.009.
[13] Popov G.A., Popov A.G. The final grade if there are several evaluation options using the example of information security problems. Bulletin of the Astrakhan State Technical University. Series: Management, Computer Engineering and Computer Science. 2017. No. 1. P. 48–61. URL: https://www.elibrary.ru/item.asp?id=28147036 (accessed: 14.04.2021).

Поступила в редакцию – 24 февраля 2021 г. Окончательный вариант – 29 апреля 2021 г.
Received – February 24, 2021. The final version – April 29, 2021.