УНИВЕРСИТЕТ ИТМО
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
май–июнь 2021 Том 21 № 3 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
May–June 2021 Vol. 21 No 3 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

doi: 10.17586/2226-1494-2021-21-3-437-441
УДК 004.056

Анализ методик оценки рисков информационной безопасности кредитно-финансовых организаций

Евгений Александрович Беляев[1]✉, Ольга Александровна Емельянова[2], Илья Иосифович Лившиц[3]

[1,2,3] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация

[1] eabeliaev@yandex.ru✉, http://orcid.org/0000-0003-1627-7066
[2] emelyanova1397@gmail.com, http://orcid.org/0000-0003-0362-7987
[3] Livshitz.il@yandex.ru, http://orcid.org/0000-0003-0651-8591

Аннотация
Представлен анализ методик оценки рисков информационной безопасности, определены их особенности, достоинства и недостатки, рассмотрено применение таких методик в кредитно-финансовых организациях. Сформированы критерии сравнения методик оценки рисков информационной безопасности, описаны их достоинства и недостатки. Показано, что несмотря на требования регуляторов к оценке рисков, большинство нормативно-правовых документов посвящено операционным рискам. Оценка рисков информационной безопасности кредитно-финансовых организаций не имеет достаточной регламентации и формализации. Обоснована необходимость разработки метода оценки рисков, учитывающего особенности, присущие кредитно-финансовым организациям. Рассмотрена потребность в создании перечней существующих угроз кредитно-финансовой сферы и их привязка к существующим уязвимостям для оптимизации процесса оценки рисков. Разработка методики оценки рисков информационной безопасности позволит повысить степень соответствия кредитно-финансовых организаций требованиям международных, государственных и отраслевых стандартов за счет оптимального набора мер защиты и моделей оценки рисков.

Ключевые слова
оценка рисков, информационная безопасность, кредитно-финансовые организации, управление рисками, платежная система

Ссылка для цитирования: Беляев Е.А., Емельянова О.А., Лившиц И.И. Анализ методик оценки рисков информационной безопасности кредитно-финансовых организаций // Научно-технический вестник информационных технологий, механики и оптики. 2021. Т. 21, № 3. С. 437–441. doi: 10.17586/2226-1494-2021-21-3-437-441

An analysis of methods for assessing information security risks of financial institutions

Evgenii A. Belyaev[1]✉, Olga A. Emelyanova[2], Ilya I. Livshitz[3]

[1,2,3] ITMO University, Saint Petersburg, 197101, Russian Federation

[1] eabeliaev@yandex.ru✉, http://orcid.org/0000-0003-1627-7066
[2] emelyanova1397@gmail.com, http://orcid.org/0000-0003-0362-7987
[3] Livshitz.il@yandex.ru, http://orcid.org/0000-0003-0651-8591

Abstract
The paper presents an analysis of the existing methods for assessing information security risks, their features, advantages and disadvantages, as well as determines the possibility of using such techniques for assessing information security risks in financial institutions. Criteria for comparing information security risk assessment methods have been formed, the advantages and disadvantages of the methods are described. It is shown that, despite the requirements of regulators for assessing information security risks, most of the regulatory documents deal with operational risks. The evaluation of information security risks of credit and financial institutions does not have sufficient regulation and formalization.

The authors substantiate the necessity of developing a method for assessing information security risks for credit and financial organizations, taking into account the features of risk assessment inherent to the mentioned organizations. The paper considers the need to create lists of existing threats to the credit and financial sector and their linking to existing vulnerabilities to optimize the process of assessing information security risks. The development of a methodology for assessing information security risks will increase the degree of compliance of credit and financial institutions with the requirements of international, state and industry standards through an optimal set of protection measures and models for evaluating information security risks.

Keywords
risk assessment, information security, financial institutions, risk management, payment system

For citation: Belyaev E.A., Emelyanova O.A., Livshitz I.I. An analysis of methods for assessing information security risks of financial institutions. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2021, vol. 21, no. 3, pp. 437–441 (in Russian). doi: 10.17586/2226-1494-2021-21-3-437-441

Развитие банковской системы напрямую связано с состоянием и уровнем информационной безопасности. В связи с непрерывно растущим числом угроз информационной безопасности, регулирующие организации постоянно совершенствуют требования, предъявляемые к организациям кредитно-финансовой системы [1].

Каждая кредитно-финансовая организация должна соответствовать требованиям Федеральных законов, государственных стандартов, нормативных актов Центрального Банка Российской Федерации (ЦБ РФ), требованиям Федеральной службы по техническому и экспортному контролю Российской Федерации (ФСТЭК России), что является трудоемкой задачей, поскольку все требования делятся на различные уровни регуляторов и не систематизированы. В отличие от других сфер деятельности, организации кредитно-финансовой сферы находятся в зоне более сложного регулирования. Требования регуляторов зачастую не имеют четких и формализованных методик [2].

В соответствии с требованиями Федерального закона от 27.06.2011 г. № 161-ФЗ[1] операторы по переводу денежных средств и банковские платежные агенты должны обеспечивать защиту информации о средствах и методах обеспечения информационной безопасности, персональных данных и иной информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации. Согласно требованиям статьи 15 указанного Федерального закона, оператор платежной системы обязан организовывать системы управления рисками в платежной системе, осуществлять оценку и управление рисками. Кроме того, в Федеральном законе в явном виде определены требования к системе управления рисками в платежной системе.

Во исполнение требований указанного Федерального закона, регулятором банковской системы Банком России подготовлено и издано Положение от 09.06.2012 г. № 382-П[2]. Указанное Положение определяет необходимость выявления угроз, рисков и уязвимостей в обеспечении защиты информации при осуществлении переводов денежных средств.

Документом[3] Базель III Базельского комитета по банковскому надзору, членом которого является Российской Федерации, определены требования к управлению кредитными и операционными рисками. Несмотря на то, что документ косвенно затрагивает риски информационной безопасности, он играет важное значение для выработки унифицированного подхода к управлению различными типами рисков.

В настоящее время документ Базель III находится на стадии внедрения. С целью перспективного использования новых стандартизированных подходов к оценке операционных рисков для расчета достаточности капиталов ЦБ РФ установил требования к системе управления операционными рисками в Положении Банка России от 08.04.2020 г. № 716-П[4]. Положение определяет требование к ведению баз данных о событии операционного риска, в том числе риска информационной безопасности.

Регулятор кредитно-финансовой системы Банк России разработал ГОСТ Р 57580.1-2017[5]. Стандарт также содержит требования к системе управления рисками в кредитно-финансовых организациях. Значительное внимание в документе уделяется операционному риску.

Исходя из проведенного анализа нормативных и иных актов Российской Федерации по обеспечению информационной безопасности кредитно-финансовой сферы, можно сделать вывод о том, что Федеральными законами, Государственными стандартами, Положениями Банка России определены требования по управлению рисками информационной безопасности кредитно-финансовых организаций. При этом все действующие в настоящее время законы, стандарты и документы регулятора посвящены в значительной степени системе управления операционным риском. Единые формализованные подходы к системе управ-

[1] Федеральный закон от 27.06.2011 г. №161-ФЗ «О национальной платежной системе».

[2] Положение от 09.06.2012 № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований по обеспечению защиты информации при осуществлении переводов денежных средств».

[3] Basel III: A global regulatory framework for more resilient banks and banking systems, Bank for International Settlements 2010.

[4] Положении Банка России от 08.04.2020 г. № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе».

[5] ГОСТ Р 57580.1-2017 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер. Введен 01.01.2018. М.: Стандартинформ, 2020. 66 с.

ления риском информационной безопасности не имеют достаточной регламентации.

Единственным документом, который определяет порядок оценки рисков информационной безопасности организаций кредитно-финансовой сферы, являются рекомендации в области стандартизации Банка России РС БР ИББС-2-2.2-2009[1]. Методика разработана в 2009 году и в последующем не актуализировалась. Документ не содержит определенный перечень рассматриваемых угроз информационной безопасности, аналогичный банку данных угроз ФСТЭК, что приводит к зависимости результатов от подходов, применяемых экспертом, проводящим оценку, и не имеет формализованного подхода к оцениваемым угрозам информационной безопасности.

К достоинствам методики оценки рисков информационной безопасности можно отнести ее непосредственную направленность на оценку рисков в кредитно-финансовых организациях. Методика включает в себя типовые формы документирования для каждой процедуры оценки рисков.

Наряду с рекомендациями по оценке рисков информационной безопасности Банка России кредитно-финансовые организации используют модели, регламентированные международными стандартами.

Широкое применение в управлении рисками информационной безопасности кредитно-финансовых организаций имеет международный стандарт ISO/IEC 27005:2018[2] «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» [3]. Под оценкой риска в терминологии указанного стандарта понимается общий процесс идентификации, анализа и оценки опасности рисков. Стандарт содержит подробную методику оценки риска и зачастую используется для формирования общего представления по организации процесса управления рисками информационной безопасности. К недостаткам стандарта можно отнести его теоретический уклон и общность формулировок. Кредитные организации выбирают сертификацию по требованиям ISO с целью получить статус, который будет признаваться во всем мире. В рамках оценки рисков информационной безопасности проводится оценка стоимости активов, идентификация актуальных угроз и уязвимостей, анализируются средства защиты, проводится оценка последствий реализации риска.

Также для оценки рисков информационной безопасности кредитно-финансовых организации эксперты нередко используют набор документов американского национального института стандартов и технологий NIST. Процедуре оценки риска информационной безопасности посвящено «Руководство по проведению оценок риска» NIST 800-30[3]. В отличие от ISO/IEC 27005, документ NIST 800-30 носит лишь рекомендательный характер, содержит более детальное описание процедур оценки рисков, а также практические рекомендации [4].

Методика оценки риска по документу NIST 800-30 включает в себя подготовку, проведение, коммуницирование результатов оценки риска и поддержание достигнутых результатов. Наряду с классическими количественным и качественным способами оценки рисков она содержит полуколичественный способ, являющийся промежуточным вариантом, который позволяет повысить точность оценки [5].

Также для оценки рисков информационной безопасности применяются иные методики, среди которых методика оценки рисков Octave. Особенность методики заключается в простоте процедуры оценки рисков, которая проводится силами сотрудников организации. При описании профиля угроз предлагается использовать деревья вариантов, что повышает наглядность оценки. За счет своей простоты методика позволяет провести только качественную оценку рисков и не позволяет в полной мере охватить бизнес-процессы кредитно-финансовых организаций и присущие им риски [6, 7].

Сравнительный анализ методик оценки рисков информационной безопасности приведен в таблице.

Существующие методики оценки рисков информационной безопасности не могут в полной мере являться эталонными для всех сфер производственной деятельности. На данный момент методики, разработанные непосредственно для построения рисковых моделей в организациях кредитно-финансовой сферы, практически полностью отсутствуют.

Также отсутствует банк данных угроз информационной безопасности организаций кредитно-финансовой сферы, что обуславливается следующими основными факторами:

— практически полное закрытие любой информации со стороны организаций банковской сферы, о возникновении любых угроз безопасности информации, с целью недопущения репутационных потерь компании;
— существенное отличие сетевой и информационной инфраструктур организаций банковской сферы от подавляющего большинства организаций других сфер в Российской Федерации, что в том числе влияет на количество и способы реализации угроз безопасности информации, применимые именно к организациям банковской сферы;
— сложность и комплексность построения систем обеспечения безопасности информации организаций банковской сферы, что делает неприменимым большинство типовых угроз безопасности информации, отраженных в банке данных угроз ФСТЭК России;
— особый контроль и требования со стороны регулирующих органов Российской Федерации по информационной безопасности всех организаций банковской сферы, с учетом важности и специфики их деятельности.

[1] Рекомендации в области стандартизации Банка России РС БР ИББС-2.2-2009 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности». Москва, 2009.

[2] Стандарт ISO/IEC 27005:2018 «Information technology — Security techniques — Information security risk management».

[3] NIST Special Publication (SP) 800-30, Revision 1, Guide for Conducting Risk Assessments

Таблица. Методики оценки рисков информационной безопасности
Table. Methods for assessing information security risks

Критерии сравнения	РС БР ИББС-2-2.2-2009	ISO/IEC 27005	NIST 800-30	OCTAVE
Характер методики	Рекомендация	Стандарт. Возможность сертификации на соответствие	Рекомендация	Рекомендация
Этапы оценки рисков	1. Определение перечня типов активов. 2. Определение перечня объектов среды. 3. Определение источников угроз. 4. Определение степени возможности реализации угрозы. 5. Определение степени последствий нарушения информационной безопасности. 6. Оценка рисков.	1. Идентификация риска. 2. Анализ рисков. 3. Оценка опасности рисков	1. Подготовительный этап. 2. Оценка рисков. 3. Коммуницирование результатов. 4. Поддержание достигнутых результатов.	1. Разработка профилей угроз. 2. Идентификация уязвимостей. 3. Разработка стратегии безопасности.
Подходы к оценке рисков	Качественный Количественный	Качественный Количественный	Качественный Количественный Полуколичественный	Качественный
Особенности методики	Методика разработана непосредственно для кредитно-финансовых организаций. Содержит типовые формы документирования результатов оценки.	Возможность получения сертификата соответствия, признаваемого мировым сообществом. Полный комплект стандартов по управлению рисками информационной безопасности	Детальный подход. Документ содержит перечни угроз и уязвимостей	Документация общедоступна и бесплатна. Оценка силами сотрудников организации

Банк данных угроз информационной безопасности организаций кредитно-финансовой сферы позволит формализовать процесс проведения оценки рисков информационной безопасности. Сформированный перечень угроз должен быть ранжирован и систематизирован, что позволит оптимизировать и в том числе ускорить процесс оценки рисков. Формирование единого централизованного банка данных угроз информационной безопасности кредитно-финансовых организаций позволит унифицировать общий подход и выработать современный, актуальный перечень возникающих угроз безопасности информации. Это приведет к существенному повышению эффективности построения рисковых моделей, за счет сокращения временных затрат на выявление и актуализацию основного перечня угроз безопасности информации для организаций банковской сферы. Подобная категория ресурсов должна иметь однозначную привязку конкретной угрозы безопасности информации, находящейся в перечне, с существующем перечнем актуальных уязвимостей в применяемых средствах и информационных технологиях. Привязка должна быть реализована в полностью автоматическом формате, так как для одной угрозы характерен целый набор сопутствующих уязвимостей, количество которых будет существенно превышать суммарные показатели количества угроз. С учетом текущего опыта ФСТЭК России на 217 угроз безопасности информации в текущем актуальном перечне банка данных угроз приходится порядка 25 697 выявленных уязвимостей, связь между которыми не установлена, что практически полностью лишает возможности эффективного применения собранной информации по уязвимостям, в контексте построения и последующей оценки угроз и рисков безопасности в организации.

Результаты выполненного анализа показали существующую потребность в создании методики оценки рисков информационной безопасности, учитывающую особенности, присущие кредитно-финансовым организациям. Методика позволит повысить степень соответствия кредитно-финансовых организаций требованиям международных, государственных и отраслевых стандартов, за счет оптимального набора мер защиты и моделей оценки рисков. Создание банка данных угроз безопасности для кредитно-финансовых организаций не только обеспечит формализацию подходов к оценке рисков, но и будет способствовать повышению соответствия кредитно-финансовых организаций требованиям документа Базель III.

Литература

1. Бердюгин А.А. Управление риском нарушения информационной безопасности в условиях электронного банкинга // Вопросы кибербезопасности. 2018. № 1. С. 28–38. doi: 10.21681/2311-3456-2018-1-28-38
2. Беляев Е.А., Емельянова О.А., Исаев А.С. Проблемы применения методических документов Банка России при осуществлении оценки рисков информационной безопасности кредитно-финансовых организаций // Научно-технический вестник Поволжья. 2020. № 4. С. 84–86.
3. Баранова Е.К., Мурзакова А.А., Мурзакова Е.А. Сравнительный анализ программного обеспечения для анализа рисков информационной безопасности в соответствии с ГОСТ Р ИСО/МЭК 27005-10 // Информационные технологии и вычислительные системы. 2019. № 2. С. 75–83. doi: 10.14357/20718632190208
4. Supriyadi Y., Hardani C.W. Information system risk scenario using COBIT 5 for risk and NIST SP 800-30 Rev. 1 a case study // Proc. 3rd International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE). Yogyakarta, Indonesia. 2018. P. 287–291. doi: 10.1109/ICITISEE.2018.8721034
5. Мищенко В.И., Шилов А.К. Управление рисками информационной безопасности в автоматизированных системах управления // Информационные системы и технологии. 2015. № 2. С. 138–142.
6. Oppliger R. Quantitative risk analysis in information security management: A modern fairy tale // IEEE Security and Privacy. 2015. V. 13. N 6. P. 18–21. doi: 10.1109/MSP.2015.118
7. Varela-Vaca Á.J., Parody L., Casca R.M., Gómez-López M.T. Automatic verification and diagnosis of security risk assessments in business process models // IEEE Access. 2019. V. 7. P. 26448–26465. doi: 10.1109/ACCESS.2019.2901408

References

1. Berdyugin A. Risk management of information security violation in conditions of electronic banking. *Voprosy kiberbezopasnosti*, 2018, no. 1, pp. 28–38. (in Russian). doi: 10.21681/2311-3456-2018-1-28-38
2. Belyaev E.A., Emelyanova O.A., Isaev A.S. Problems of applying the metodological documents of the Bank of Russia in assessing information security risks of financial institutions. *Scientific and Technical Volga region Bulletin*, 2020, no. 4, pp. 84–86. (in Russian)
3. Baranova E.C., Murzakova A.A., Murzakova E.A. Modern software tools for information security risks management ISO/IEC 27005. *Journal of Information Technologies and Computing Systems*, 2019, no. 2, pp. 75–83. (in Russian). doi: 10.14357/20718632190208
4. Supriyadi Y., Hardani C.W. Information system risk scenario using COBIT 5 for risk and NIST SP 800-30 Rev. 1 a case study. *Proc. 3rd International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*. Yogyakarta, Indonesia, 2018, pp. 287–291. doi: 10.1109/ICITISEE.2018.8721034
5. Mishhenko V.I., Shilov A.K. Risk management information security in automated systems management. *Information Systems and Technologies*, 2015, no. 2, pp. 138–142. (in Russian)
6. Oppliger R. Quantitative risk analysis in information security management: A modern fairy tale. *IEEE Security and Privacy*, 2015, vol. 13, no. 6, pp. 18–21. doi: 10.1109/MSP.2015.118
7. Varela-Vaca Á.J., Parody L., Casca R.M., Gómez-López M.T. Automatic verification and diagnosis of security risk assessments in business process models. *IEEE Access*, 2019, vol. 7, pp. 26448–26465. doi: 10.1109/ACCESS.2019.2901408

Авторы

Беляев Евгений Александрович — аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, http://orcid.org/0000-0003-1627-7066, eabeliaev@yandex.ru
Емельянова Ольга Александровна — аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, http://orcid.org/0000-0003-0362-7987, emelyanova1397@gmail.com
Лившиц Илья Иосифович — доктор технических наук, профессор практики, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, SC 57191569306, http://orcid.org/0000-0003-0651-8591, Livshitz.il@yandex.ru

Authors

Evgenii A. Belyaev — Postgraduate, ITMO University, Saint Petersburg, 197101, Russian Federation, http://orcid.org/0000-0003-1627-7066, eabeliaev@yandex.ru
Olga A. Emelyanova — Postgraduate, ITMO University, Saint Petersburg, 197101, Russian Federation, http://orcid.org/0000-0003-0362-7987, emelyanova1397@gmail.com
Ilya I. Livshitz — D.Sc., Full Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, SC 57191569306, http://orcid.org/0000-0003-0651-8591, Livshitz.il@yandex.ru

Статья поступила в редакцию 18.03.2021
Одобрена после рецензирования 09.04.2021
Принята к печати 11.05.2021

Received 18.03.2021
Approved after reviewing 09.04.2021
Accepted 11.05.2021