www.volsu.ru

CC BY

DOI: https://doi.org/10.15688/NBIT.jvolsu.2025.1.2

УДК 621.39(043)
ББК 32.88я43

ОЦЕНКА РИСКОВ ВОЗНИКНОВЕНИЯ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ

Владислав Георгиевич Яриков

Кандидат педагогических наук, доцент,
кафедра методики преподавания математики и физики, ИКТ,
Волгоградский государственный социально-педагогический университет
yarikov_vg@mail.ru
просп. им. В.И. Ленина, 27, 400005 г. Волгоград, Российская Федерация

Виталий Алексеевич Ревунов

Студент, кафедра информационной безопасности,
Волгоградский государственный университет
ibb-192_876241@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В статье рассматриваются современные подходы к оценке рисков в области кибербезопасности. В условиях стремительного развития технологий и увеличения числа киберугроз эффективное управление рисками становится критически важным для организаций всех размеров. Авторы анализируют основные методологии и инструменты, используемые для оценки и управления рисками, включая рамочные программы, такие как NIST Cybersecurity Framework и рекомендации ENISA. Особое внимание уделяется актуальным угрозам, выявленным в последних отчетах, и практическим шагам, которые организации могут предпринять для повышения своей киберустойчивости. Статья предназначена для специалистов в области кибербезопасности, руководителей и менеджеров, стремящихся улучшить свои знания и навыки в управлении рисками, а также для исследователей, интересующихся последними тенденциями и вызовами в данной области.

Ключевые слова: кибербезопасность, управление рисками, оценка рисков, NIST Cybersecurity Framework, киберугрозы.

© Яриков В.Г., Ревунов В.А., 2025

В условиях стремительного развития цифровых технологий и увеличения зависимости общества от информационных систем, вопросы кибербезопасности приобретают особую актуальность. Современные организации сталкиваются с растущим числом компьютерных инцидентов, включая кибератаки, утечки данных и вредоносные программы, которые способны нанести значительный ущерб как финансовым, так и репутационным активам. По данным различных исследований, количество кибератак в последние годы возросло в несколько раз, что подчеркивает необходимость разработки эффективных стратегий по их предотвращению и минимизации последствий.

Актуальность оценки рисков возникновения компьютерных инцидентов обусловлена не только возросшей частотой атак, но и их раз-

нообразием и сложностью. Киберпреступники используют все более изощренные методы, что делает традиционные подходы к безопасности недостаточно эффективными. По этой причине организациям необходимо внедрять системный подход к управлению рисками, который включает в себя как технические, так и организационные меры.

Цель данного исследования – проанализировать существующие методы оценки рисков и предложить рекомендации по их улучшению. В рамках исследования мы стремимся ответить на следующие вопросы: какие подходы наиболее эффективны для оценки рисков? Как можно улучшить существующие методологии, чтобы они лучше соответствовали современным вызовам информационной безопасности?

Методологии оценки рисков

В современных условиях информационной безопасности существует множество методик, которые помогают организациям анализировать и управлять рисками, связанными с компьютерными инцидентами. Каждая из этих методик предлагает свой уникальный способ выявления, анализа и снижения рисков.

NIST (Национальный институт стандартов и технологий). Методология NIST, особенно ее известный специальный выпуск NIST SP 800-30, предоставляет рекомендации по управлению рисками в сфере информационной безопасности. Этот подход выделяется своей универсальностью и адаптивностью, что позволяет ему быть применимым в различных организационных контекстах. NIST предлагает всесторонний процесс, который включает в себя идентификацию активов, угроз и уязвимостей, а также оценку вероятности и последствий потенциальных инцидентов. Однако реализация данной методологии может потребовать значительных ресурсов, включая время и финансовые затраты, для обеспечения ее эффективного функционирования [5].

OCTAVE (Оценка операционно критических угроз, активов и уязвимостей). Методология OCTAVE сосредоточена на операционных рисках и предназначена для организаций, стремящихся интегрировать управление рисками в свои бизнес-процессы. OCTAVE предлагает структурированный подход к выявлению критически важных активов и оценке связанных с ними угроз и уязвимостей. Этот метод позволяет организациям выявлять и приоритизировать риски в зависимости от их влияния на операционные процессы. Тем не менее OCTAVE может оказаться менее эффективной для анализа стратегических угроз, таких как долгосрочные изменения в сфере киберугроз [6].

FAIR (Анализ факторов информационных рисков). Методология FAIR предлагает количественный подход к оценке рисков, что позволяет организациям более точно определять потенциальные убытки от компьютерных инцидентов. FAIR основывается на анализе факторов, влияющих на риски, и использует математические модели для оценки вероятности и последствий инцидентов. Этот подход требует наличия точных данных для анализа, что может стать вызовом для организаций, у которых нет достаточного объема исторических данных. Тем не менее FAIR предоставляет ценные инструменты для принятия обоснованных решений в области управления рисками [3].

Сравнение и выбор подхода

Выбор подходящей методологии для оценки рисков обусловлен множеством факторов, включая размер и специфику организации, доступные ресурсы и конкретные цели в области управления рисками. Организациям следует учитывать свои уникальные требования и контекст, чтобы выбрать метод, который наилучшим образом соответствует их потребностям.

При выборе подхода важно учитывать не только текущие потребности, но и возможность адаптации методологии к будущим изменениям в сфере киберугроз. В условиях быстро меняющегося кибербезопасного ландшафта может потребоваться более гибкий и адаптивный подход, который позволит организациям оперативно реагировать на новые угрозы.

Практическое применение методологий

После выбора подходящей методологии оценки рисков организациям необходимо пе-

рейти к ее практической реализации. Этот процесс включает несколько ключевых этапов, которые помогут обеспечить эффективное управление рисками и повысить уровень информационной безопасности.

Этап 1: Идентификация активов и угроз. Первый шаг в любом процессе оценки рисков заключается в выявлении критически важных активов организации, таких как данные, системы и инфраструктура. Понимание того, какие активы наиболее ценны для бизнеса, позволяет сосредоточить усилия на их защите. Важно также выявить потенциальные угрозы, которые могут повлиять на эти активы, включая как внешние угрозы (например, кибератаки), так и внутренние (например, ошибки сотрудников).

Этап 2: Анализ уязвимостей. После идентификации активов и угроз следует провести анализ уязвимостей. Этот этап включает оценку слабых мест в системах и процессах, которые могут быть использованы злоумышленниками для нанесения ущерба. Организации могут применять различные инструменты и методы, такие как сканирование уязвимостей и тестирование на проникновение, для выявления и оценки уязвимостей.

Этап 3: Оценка вероятности и воздействия. На этом этапе организации должны оценить вероятность реализации каждой угрозы и ее потенциальное воздействие на бизнес. Это можно сделать как качественными, так и количественными методами, в зависимости от выбранной методологии. Например, методология FAIR предлагает использовать статистические модели для более точной оценки вероятности и последствий инцидентов.

Этап 4: Разработка и внедрение мер по снижению рисков. На основе проведенного анализа организации должны разработать стратегии и меры по снижению выявленных рисков. Это может включать как технические меры, такие как установка систем обнаружения вторжений, так и организационные меры, например, обучение сотрудников и разработка политик безопасности. Важно, чтобы эти меры были соразмерны уровню риска и соответствовали ресурсам организации.

Этап 5: Мониторинг и пересмотр. Управление рисками – это непрерывный процесс, требующий регулярного мониторинга и пересмотра. Организации должны постоянно отслеживать изменения в ландшафте угроз и адаптировать свои стратегии управления рисками в соответствии с новыми вызовами. Регулярные аудиты и тестирования помогут оценить эффективность внедренных мер и выявить области для улучшения [1].

Внедрение культуры безопасности. Формирование культуры безопасности в организации является одним из ключевых аспектов успешного управления рисками. Это включает не только технические меры, но и активное вовлечение всех сотрудников в процесс обеспечения информационной безопасности.

Обучение и повышение осведомленности. Обучение сотрудников является основой для создания культуры безопасности. Регулярные тренинги и семинары по кибербезопасности помогают работникам распознавать потенциальные угрозы, такие как фишинговые атаки, и правильно на них реагировать. Повышение осведомленности о рисках и методах их предотвращения способствует снижению вероятности инцидентов, связанных с человеческим фактором.

Разработка и внедрение политик безопасности. Четко определенные политики безопасности играют важную роль в управлении рисками. Они должны охватывать все аспекты работы с информацией, включая доступ к данным, использование корпоративных устройств и работу с удаленными системами. Политики безопасности должны быть легко доступными и понятными для всех сотрудников, а также регулярно пересматриваться и обновляться в соответствии с изменяющимися угрозами.

Вовлечение руководства. Поддержка и активное участие руководства в вопросах информационной безопасности критически важны для успешного внедрения культуры безопасности. Руководители должны демонстрировать приверженность высоким стандартам безопасности и поощрять сотрудников следовать установленным политикам и процедурам. Это помогает создать атмосферу доверия и ответственности в организации.

Технологические решения и инновации. Технологические инновации играют решающую роль в минимизации рисков, связанных с компьютерными инцидентами. Совре-

менные инструменты и технологии способствуют автоматизации процессов управления рисками, обеспечивая более надежную защиту.

Применение искусственного интеллекта и машинного обучения. Искусственный интеллект и машинное обучение становятся ключевыми инструментами в сфере кибербезопасности. Они позволяют обрабатывать большие объемы данных и выявлять аномалии, которые могут указывать на потенциальные угрозы. Эти технологии помогают организациям быстрее реагировать на инциденты и уменьшать их последствия.

Внедрение систем мониторинга и обнаружения. Современные системы мониторинга и обнаружения угроз помогают организациям оперативно идентифицировать и реагировать на инциденты. Эти системы способны автоматически уведомлять ответственных сотрудников о подозрительной активности и предоставлять детальную информацию для дальнейшего анализа. Внедрение таких систем значительно повышает уровень безопасности и снижает риск успешных атак.

Влияние человеческого фактора на управление рисками

Человеческий фактор остается одним из самых важных аспектов в управлении рисками. Сотрудники могут как повышать уровень безопасности, так и представлять собой потенциальные уязвимости.

Формирование понимания и ответственности

Создание культуры осведомленности и ответственности среди сотрудников является важным компонентом управления рисками. Это включает в себя систематический подход к обучению и повышению осведомленности о рисках, акцентируя внимание на важности соблюдения политик безопасности. Сотрудники должны не только осознавать свою роль в защите корпоративных данных, но и активно участвовать в этом процессе, следуя установленным стандартам и процедурам. Введение механизмов поощрения за соблюдение норм безопасности может значительно повысить мотивацию и ответственность персонала.

Поддержка и развитие компетенций

Организациям следует инвестировать в развитие навыков своих сотрудников в области кибербезопасности. Это может включать как внутренние тренинги, так и участие в внешних курсах и сертификационных программах. Развитие профессиональных навыков сотрудников способствует более эффективному управлению рисками и повышению общей устойчивости организации [2; 4].

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р ИСО/МЭК 27001-2014 – Информационная технология. Методы и средства обеспечения безопасности. Системы управления информационной безопасностью. Требования. – М. : Стандартинформ, 2014. – 36 с. – URL: https://docs.cntd.ru/document/1200170125

2. Козырь, Н. С. Методические подходы риск-менеджмента информационной безопасности / Н. С. Козырь. – Научные труды КубГТУ. – 2023. – № 4. – С. 99–109.

3. Freund, J. Measuring and Managing Information Risk: A FAIR Approach / J. Freund, J. Jones. – Hoboken : Wiley, 2015. – 320 p.

4. ISO 31000:2018. Risk Management – Guidelines. – Geneva : International Organization for Standardization, 2018. – URL: https://pqm-online.com/assets/files/pubs/translations/std/iso-31000-2018-(rus).pdf

5. Joint Task Force Transformation Initiative National Institute of Standards and Technology. Guide for Conducting Risk Assessments. – Gaithersburg : NIST, 2012. – DOI: 10.6028/NIST.SP.800-30r1

6. Tucker B. Advancing Risk Management Capability Using the OCTAVE FORTE Process. – Pittsburgh, Carnegie Mellon University, 2020. – 106 p. – DOI: 10.1184/R1/13014266.v1

REFERENCES

1. *GOST R ISO/IEC 27001-2014 – Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Sistemy upravleniya informatsionnoy bezopasnostyu. Trebovaniya* [GOST R ISO/IEC 27001-2014 – Information Technology. Security Techniques. Information Security

Management Systems. Requirements]. Moscow, Standartinform, 2014. 36 p. URL: https://docs.cntd.ru/document/1200170125

2. Kozyr N.S. Metodicheskie podkhody risk-menedzhmenta informatsionnoy bezopasnosti [Methodological Approaches to Information Security Risk Management]. *Nauchnye trudy KubGTU* [Scientific Works of KubSTU], 2023, no. 4, pp. 99-109. URL: https://ntk.kubstu.ru/data/mc/0100/4667.pdf

3. Freund J., Jones J. *Measuring and Managing Information Risk: A FAIR Approach*. Hoboken, Wiley, 2015. 320 p.

4. *ISO 31000:2018. Risk Management – Guidelines*. Geneva, International Organization for Standardization, 2018. URL: https://pqm-online.com/assets/files/pubs/translations/std/iso-31000-2018-(rus).pdf

5. *Joint Task Force Transformation Initiative National Institute of Standards and Technology. Guide for Conducting Risk Assessments*. Gaithersburg, NIST, 2012. DOI: 10.6028/NIST.SP.800-30r1

6. Tucker B. *Advancing Risk Management Capability Using the OCTAVE FORTE Process*. Pittsburgh, Carnegie Mellon University, 2020. 106 p. DOI: 10.1184/R1/13014266.v1

RISK ASSESSMENT OF OCCURRENCE COMPUTER INCIDENTS

Vladislav G. Yarikov

Candidate of Sciences (Pedagogy), Associate Professor,
Department of Teaching Methods of Mathematics and Physics, ICT,
Volgograd State Socio-Pedagogical University
yarikov.vladislav@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Vitaly A. Revunov

Student, Department of Information Security,
Volgograd State University
ibb-192_876241@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. This article explores contemporary methodologies for risk assessment associated with computer incidents in the field of cybersecurity. The study highlights the growing importance of effective risk management due to the rapid advancement of technology and the increasing frequency of cyber threats. The authors analyze prominent frameworks, emphasizing their unique approaches to identifying, evaluating, and mitigating risks. The article underscores the adaptability of NIST, the operational focus of OCTAVE, and the quantitative precision of FAIR, while also noting their respective limitations, such as resource intensity or data dependency. Practical implementation steps are outlined, including asset identification, vulnerability analysis, risk evaluation, and the development of mitigation strategies. The authors stress the need for continuous monitoring and adaptation to address evolving threats. Additionally, the article highlights the critical role of fostering a security culture within organizations through employee training, clear policies, and leadership involvement. Technological innovations like artificial intelligence and machine learning are presented as valuable tools for enhancing threat detection and response. The study concludes by addressing the human factor, advocating for increased awareness and competency development among staff to minimize risks. Targeted at cybersecurity professionals, managers, and researchers, the article provides actionable insights and methodologies to strengthen organizational cyber resilience in an increasingly complex threat landscape.

Key words: cybersecurity, risk management, risk assessment, NIST Cybersecurity Framework, cyber threats.