MINISTRY OF SCIENCE AND HIGHER EDUCATION OF THE REPUBLIC OF KAZAKHSTAN

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ КАЗАХСТАН

KAZAKHSTAN

ХАЛЫҚАРАЛЫҚ УНИВЕРСИТЕТІ — INTERNATIONAL UNIVERSITY — SINCE 2009 — МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Published since 2020.
Volume 7. 1 (25). 2026
January–March

ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

2020 жылдан бері шығарылады
Том 7. 1 (25). 2026
Қаңтар-Наурыз

МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Издается с 2020 г.
Том 7. 1 (25). 2026
Январь-Март

Свидетельство о постановке на учет периодического печатного издания в Министерство информации и общественного развития Республики Казахстан № KZ82VPY00020475, выданное от 20.02.2020 г.

Зарегистрировано в Международном центре регистрации серийных изданий ISSN (ЮНЕСКО, Париж, Франция). ISSN 2708–2032 (print), ISSN 2708–2040 (online)

Журнал входит в Перечень научных изданий, рекомендуемых КОКНВО МНВО РК для публикации основных результатов научной деятельности.

International Journal of Information and Communication Technologies
Periodicity: 4 times a year.
Languages: Kazakh, Russian, English
DOI prefix: 10.54309
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Thematic focus: "Information technology"; "Digital technologies in the development of socio-economic systems"; "Information security and communication technologies".

Journal website: https://journal.iitu.edu.kz
Owner: International Information Technology University JSC (Almaty).

Халықаралық ақпараттық және коммуникациялық технологиялар журналы
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Префикс DOI: 10.54309
Мерзімділігі: жылына 4 рет.
Басылым тілі: қазақ, орыс, ағылшын.
Тақырып бағыты: "Ақпараттық технологиялар"; "Ақпараттық қауіпсіздік және коммуникациялық технологиялар"; "Әлеуметтік-экономикалық жүйелерді дамытудағы цифрлық технология".
Журнал сайты: https://journal.iitu.edu.kz

Меншік иесі: АҚ «Халықаралық ақпараттық технологиялар университеті» (Алматы қ.).

Международный журнал информационных и коммуникационных технологий
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Префикс DOI: 10.54309
Периодичность: 4 выпусков в год.
Язык издания: казахский, русский, английский.
Тематическая направленность: "Информационные технологии"; "Информационная безопасность и коммуникационные технологии"; "Цифровые технологии в развитии социо-экономических систем".
Сайт журнала: https://journal.iitu.edu.kz

Собственник: АО «Международный университет информационных технологий» (г. Алматы).

CONTENTS

DIGITAL TECHNOLOGIES IN THE DEVELOPMENT OF SOCIO-ECONOMIC SYSTEMS

INFORMATION TECHNOLOGY

INFORMATION SECURITY AND COMMUNICATION TECHNOLOGIES

МАЗМҰНЫ

ӘЛЕУМЕТТІК-ЭКОНОМИКАЛЫҚ ЖҮЙЕЛЕРДІ ДАМЫТУДАҒЫ ЦИФРЛЫҚ ТЕХНОЛОГИЯЛАР

АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР

СОДЕРЖАНИЕ

ЦИФРОВЫЕ ТЕХНОЛОГИИ В РАЗВИТИИСОЦИО-ЭКОНОМИЧЕСКИХ СИСТЕМ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

INFORMATION SECUTITY AND COMMUNICATION TECHNOLOGIES
АҚПАРАТТЫҚ ҚАУІПСІЗДІК ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАРҒА АРНАЛҒАН
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Vol. 7. Is.1. Number 25 (2026). Pp. 244–269
Journal homepage: https://journal.iitu.edu.kz
https://doi.org/10.54309/IJICT.2026.25.1.016

SYSTEMATIC ANALYSIS OF RISK ASSESSMENT METHODS AND MODELS IN INFORMATION SECURITY

S.A. Adilzhanova, M.Zh. Sakypbekova, L.Sh. Cherikbaeva, G.A. Tyulepberdinova, G.T. Zhubanysheva*
Al-Farabi Kazakh National University, Almaty, Kazakhstan.
E-mail: zhubanysheva03@bk.ru

Saltanat A. Adilzhanova — PhD, Acting Associate Professor, Department of Cybersecurity and Cryptology, Faculty of Information Technologies, Al-Farabi Kazakh National University
E-mail: asaltanat81@gmail.com. https://orcid.org/0000-0003-1768-064X;
Meruert Zh. Sakypbekova — PhD, Acting Associate Professor, Department of Artificial Intelligence and Big Data, Faculty of Information Technologies, Al-Farabi Kazakh National University
E-mail: sakypbekovamerueryert@gmail.com. https://orcid.org/0000-0002-6652-1357;
Lyaylya Sh. Cherikbayeva — PhD, Associate Professor, Department of Computer Sciences, Faculty of Information Technologies, Al-Farabi Kazakh National University
E-mail: cherikbayeva.lyaylya@gmail.com. https://orcid.org/0000-0001-8948-4205;
Gulnur A. Tyulepberdinova — Candidate of Physical and Mathematical Sciences, Associate Professor, Department of Artificial Intelligence and Big Data, Faculty of Information Technologies, Al-Farabi Kazakh National University
E-mail: tyulepberdinova@gmail.com. https://orcid.org/0000-0002-4322-8983;
Guldana T. Zhubanysheva — Master's student, Department of Cybersecurity and Cryptology, Faculty of Information Technologies, Al-Farabi Kazakh National University
E-mail: zhubanysheva03@bk.ru. https://orcid.org/0009-0008-0620-4879.

Abstract. This article provides a comprehensive analysis of risk assessment methods and models in the field of information security. The study is relevant in the context of modern digital infrastructure, as cyber threats are increasing daily. The purpose of the work is to systematize the main approaches to information security risk assessment, conduct a comparative analysis based on effectiveness criteria, and demonstrate their practical application. The study describes qualitative and quantitative methods, as well as international models such as FAIR, OCTAVE, and NIST SP 800-30. A comparative analysis of methods was conducted across five criteria: accuracy, scalability, labor intensity, automation capability, and reproducibility. Experimental results are presented: automated network scanning using Nmap and OpenVAS, Monte Carlo loss simulation, and network anomaly classification using a Random Forest model (94.7% accuracy on the NSL-KDD dataset). The authors conclude that the combined application of quantitative methods and automation tools provides the most effective information security risk assessment.

Keywords: information security, risk assessment, threats, vulnerabilities, SIEM, OpenVAS, ISO/IEC 27005

For citations: S.A. Adilzhanova, M.Zh. Sakypbekova, L.Sh. Cherikbaeva, G.A. Tyulepberdinova, G.T. Zhubanysheva (2026). Systematic analysis of risk assessment methods and models in information security // International journal of information and communication technologies. Vol. 7. No. 25. Pp. 244–269. https://doi.org/10.54309/IJICT.2026.25.1.016. (In Russ.).

Conflict of interest: The authors declare that there is no conflict of interest.

АҚПАРАТТЫҚ ҚАУІПСІЗДІКТЕ ТӘУЕКЕЛДЕРДІ БАҒАЛАУ ӘДІСТЕРІ МЕН МОДЕЛЬДЕРІН ЖҮЙЕЛІ ТАЛДАУ

С.А. Адилжанова, М.Ж. Сакыпбекова, Л.Ш. Черикбаева, Г.А. Тюлепбердинова, Г.Т. Жубанышева*

Әл Фараби атындағы Қазақ Ұлттық Университеті, Қазақстан, Алматы.
E-mail: zhubanysheva03@bk.ru

Адилжанова Салтанат — PhD, Әл-Фараби атындағы Қазақ Ұлттық Университеті ақпараттық технологиялар факультеті “киберқауіпсіздік және криптология” кафедрасының доцентінің м.а.
E-mail: asaltanat81@gmail.com. https://orcid.org/0000-0003-1768-064X;
Сакыпбекова Меруерт — PhD, Әл-Фараби атындағы Қазақ Ұлттық Университеті ақпараттық технологиялар факультеті “жасанды интелект жане Big Data” кафедрасының доцентінің м.а.
E-mail: sakypbekovameruyert@gmail.com. https://orcid.org/0000-0002-6652-1357;
Черикбаева Ляйля — PhD, Әл-Фараби атындағы Қазақ Ұлттық Университеті ақпараттық технологиялар факультеті “компьютерлік ғылымдар” кафедрасының қауымдастырылған профессоры

E-mail: cherikbayeva.lyailya@gmail.com. https://orcid.org/0000-0001-8948-4205;
Тюлепбердинова Гулнур — физика-математика ғылымдарының кандидаты, Әл-Фараби атындағы Қазақ Ұлттық Университеті ақпараттық технологиялар факультеті "жасанды интелект жане Big Data" кафедрасының қауымдастырылған профессоры
E-mail: tyulepberdinova@gmail.com. https://orcid.org/0000-0002-4322-8983;
Жубанышева Гулдана — Әл-Фараби атындағы Қазақ Ұлттық Университеті ақпараттық технологиялар факультеті "киберқауіпсіздік және криптология" кафедрасының магистранты
E-mail: zhubanysheva03@bk.ru. https://orcid.org/0009-0008-0620-4879.

Аннотация. Бұл мақалада ақпараттық қауіпсіздік саласындағы тәуекелдерді бағалау әдістері мен модельдеріне жан-жақты талдау жасалады. Зерттеу тақырыбы қазіргі заманғы цифрлық инфрақұрылым жағдайында өзекті болып табылады. Жұмыстың мақсаты – ақпараттық қауіпсіздік тәуекелдерін бағалаудың негізгі тәсілдерін жүйелеу, оларды тиімділік критерийлері бойынша салыстырмалы талдау жүргізу және практикалық қолданылуын көрсету. Зерттеу барысында сапалық және сандық әдістер, сондай-ақ FAIR, OCTAVE, NIST SP 800-30 секілді халықаралық модельдер сипатталған. Әдістердің бес критерий бойынша салыстырмалы талдауы жүргізілді: дәлдік, масштабталу, еңбек сыйымдылығы, автоматтандыру мүмкіндігі және қайталану. Эксперимент нәтижелері ұсынылды: Nmap және OpenVAS көмегімен желіні автоматтандырылған сканерлеу, Монте-Карло әдісімен шығындарды модельдеу, сондай-ақ Random Forest моделі арқылы желілік аномалияларды жіктеу (NSL-KDD деректер жинағында 94,7% дәлдік). Нәтижесінде, авторлар сандық әдістер мен автоматтандыру құралдарын біріктіріп қолдану ақпараттық қауіпсіздік тәуекелдерін тиімді бағалауды қамтамасыз ететінін негіздейді.

Түйін сөздер: ақпараттық қауіпсіздік, тәуекелдерді бағалау, қауіптер, осалдықтар, SIEM, OpenVAS, ISO/IEC 27005

Дәйексөздер үшін: С.А. Адилжанова, М.Ж. Сакыпбекова, Л.Ш. Черикбаева, Г.А. Тюлепбердинова, Г.Т. Жубанышева (2026). Ақпараттық қауіпсіздікте тәуекелдерді бағалау әдістері мен модельдерін жүйелі талдау // Халықаралық ақпараттық және коммуникалық технологиялар журналы. Т. 7. №. 25. Б. 244–269 бет. https://doi.org/10.54309/IJICT.2026.25.1.016. (Орыс тіл.).

Мүдделер қақтығысы: Авторлар осы мақалада мүдделер қақтығысы жоқ деп мәлімдейді.

СИСТЕМАТИЧЕСКИЙ АНАЛИЗ МЕТОДОВ И МОДЕЛЕЙ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

С.А. Адилжанова, М.Ж. Сакыпбекова, Л.Ш. Черикбаева, Г.А. Тюлепбердинова,

Г.Т. Жубанышева*[1]
Казахский национальный университет имени аль-Фараби, Казахстан, Алматы.
E-mail: zhubanysheva03@bk.ru

Адилжанова Салтанат — кандидат технических наук, и.о. доцента кафедры «Кибербезопасность и криптология» факультета информационных технологий Казахского национального университета имени аль-Фараби
E-mail: asaltanat81@gmail.com. https://orcid.org/0000-0003-1768-064X;
Сакыпбекова Меруерт — доктор PhD, и.о. доцента кафедры «Искусственный интеллект и большие данные» факультета информационных технологий Казахского национального университета имени аль-Фараби
E-mail: sakypbekovameruyert@gmail.com. https://orcid.org/0000-0002-6652-1357;
Черикбаева Ляйля — кандидат технических наук, доцент кафедры «Компьютерные науки» факультета информационных технологий Казахского национального университета имени аль-Фараби
E-mail: cherikbayeva.lyailya@gmail.com. https://orcid.org/0000-0001-8948-4205;
Тюлепбердинова Гульнур — кандидат физико-математических наук, доцент кафедры «Искусственный интеллект и большие данные» факультета информационных технологий Казахского национального университета имени аль-Фараби
E-mail: tyulepberdinova@gmail.com. https://orcid.org/0000-0002-4322-8983;
Жубанышева Гулдана — магистрант кафедры кибербезопасности и криптологии факультета информационных технологий Казахского национального университета имени аль-Фараби
E-mail: zhubanysheva03@bk.ru. https://orcid.org/0009-0008-0620-4879.

Аннотация. В данной статье представлен комплексный анализ методов и моделей оценки рисков в области информационной безопасности. Тема исследования актуальна в контексте современной цифровой инфраструктуры, поскольку киберугрозы растут с каждым днем. Цель работы – систематизировать основные методы оценки рисков информационной безопасности, провести их сравнительный анализ по критериям эффективности и продемонстрировать практическое применение. В исследовании описаны качественные и количественные методы, а также международные модели, такие как FAIR, OCTAVE и NIST SP 800-30. Проведён сравнительный анализ методов по пяти критериям: точность, масштабируемость, трудоёмкость, автоматизируемость и повторяемость. Представлены результаты экспериментов: автоматизированное сканирование сети с помощью Nmap и OpenVAS, симуляция убытков методом Монте-Карло, а также классификация сетевых аномалий с помощью модели Random Forest (точность 94,7% на датасете NSL-KDD). Авторы приходят к выводу, что комбинированное использование количественных методов и инструментов

автоматизации позволяет обеспечить наиболее эффективную и обоснованную оценку рисков информационной безопасности.

Ключевые слова: информационная безопасность, оценка рисков, угрозы, уязвимости, SIEM, OpenVAS, ISO/IEC 27005

Для цитирования: С.А. Адилжанова, М.Ж. Сакыпбекова, Л.Ш. Черикбаева, Г.А. Тюлепбердинова, Г.Т. Жубанышева (2026). Систематический анализ методов и моделей оценки рисков информационной безопасности // Международный журнал информационных и коммуникационных технологий. Том. 7. № 25. Стр. 244–269. https://doi.org/10.54309/IJICT.2026.25.1.016. (На Русс.).

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Введение.

Информационная безопасность (ИБ) является критически важным элементом для функционирования любой организации, использующей цифровые технологии и данные. Одним из важнейших аспектов ИБ является оценка рисков, которая позволяет не только выявить потенциальные угрозы и уязвимости, но и разработать соответствующие меры защиты. В условиях быстро развивающихся технологий и постоянно меняющейся ландшафта угроз оценка рисков ИБ становится все более актуальной (Плетнев и др., 2021).

Методы и модели, используемые для оценивания рисков информационной безопасности, разрабатываются с целью предсказать возможные угрозы, определить уровень их критичности и предложить оптимальные методы минимизации ущерба (Корченко и др., 2013). Эти процессы включают как количественные, так и качественные подходы, каждый из которых обладает своими преимуществами и недостатками.

Цель данной работы — рассмотреть основные методы и модели оценки рисков, а также их применение на практике для обеспечения надлежащего уровня информационной безопасности. В ходе исследования будут рассмотрены как общие принципы, так и специфические методики, применимые в различных организационных и технологических контекстах.

Формализованная постановка задачи: пусть множество методов оценки рисков ИБ обозначим как $M = \{m_1, m_2, ..., m_n\}$, а множество критериев эффективности — как $C = \{c_1, c_2, ..., c_k\}$. Задача состоит в определении функции $f: M \times C \rightarrow R$, позволяющей количественно сопоставить методы по заданным критериям и выбрать оптимальный подход для конкретного организационного контекста.

Гипотеза исследования: комбинированное применение количественных и качественных методов оценки рисков, подкреплённое автоматизированными инструментами (OpenVAS, SIEM), обеспечивает более точную и оперативную оценку рисков ИБ по сравнению с применением отдельных методов.

Материалы и методы.

Основные концепции оценки рисков в информационной безопасности

Прежде чем перейти к детальному рассмотрению методов и моделей, необходимо понять базовые концепции и термины, связанные с оценкой рисков в ИБ.

Угроза - любое событие или обстоятельство, которое может причинить вред информационным активам, нарушить их конфиденциальность, целостностьили доступность. Примерами могут быть хакерские атаки, вредоносные программы, ошибки пользователей или физические воздействия, такие как пожар или наводнение.

Уязвимость — это слабое место в системе защиты, которое может быть использовано злоумышленниками для реализации угрозы. Уязвимости могут быть как техническими (например, неисправности в программном обеспечении), так и организационными (например, недостаточная осведомленность сотрудников о вопросах ИБ).

Актив- информационный актив включает в себя как данные (например, базы данных с конфиденциальной информацией), так и системы и инфраструктуру, обеспечивающую их обработку и хранение.

Риск — вероятность того, что угроза, используя уязвимость, нанесет ущерб информационным активам. Оценка рисков предполагает анализ вероятности реализации угрозы и возможного ущерба от неё (Миков и др., 2024).

Теперь, когда основные термины определены, перейдём к методам и моделям оценки рисков.

Методы оценки рисков.

Качественные методы.

Качественные методы основаны на субъективной оценке вероятности и последствий различных угроз. Эти методы часто используются в ситуациях, когда невозможно точно измерить риск количественными показателями, и они основываются на экспертных оценках и опыте.

Метод анкетирования и интервьюирования. Один из самых распространённых методов, при котором эксперты в области ИБ опрашиваются на предмет существующих угроз и уязвимостей. На основе их ответов формируются оценки рисков, обычно выраженные в виде рейтингов (высокий, средний, низкий).

SWOT-анализ. Применяется для оценки рисков на стратегическом уровне. В рамках этого метода оцениваются сильные и слабые стороны организации, а также внешние угрозы и возможности. В контексте ИБ SWOT-анализ помогает выявить ключевые уязвимости и возможные атаки (Максименко В. Н. и др., 2017).

Количественные методы.

Количественные методы оценки рисков основаны на сборе и анализе числовых данных, что позволяет более точно оценить вероятности угроз и возможные убытки. Эти методы требуют тщательного анализа и часто используются в крупных организациях, где существует доступ к значительным объемам данных для анализа.

Метод Монте-Карло. Этот метод использует вероятностное моделирование для оценки рисков. В рамках метода создается множество возможных сценариев, каждый из которых моделируется случайным образом на основе определенных входных данных (например, частоты реализации угрозы и размера возможных убытков). В результате получается распределение вероятностей для различных исходов, что помогает лучше оценить риск и подготовиться к нему.

Метод анализа дерева отказов (FTA) (Иванченко П. Ю. и др., 2013). Данный метод предназначен для анализа причин отказов системы и выявления связей между отдельными компонентами системы, которые могут привести к сбою. На основе дерева отказов можно определить вероятность того, что определенная комбинация событий приведет к отказу системы, и оценить риски, связанные с этим отказом.

Метод анализа сценариев. В данном подходе используются данные о предыдущих инцидентах и моделирование различных сценариев для оценки возможных последствий реализации угроз. Организация рассматривает наиболее вероятные и критичные сценарии развития событий и оценивает, как различные меры безопасности могут снизить уровень риска.

Методология FAIR (Factor Analysis of Information Risk)

FAIR — это методологический подход для количественной оценки рисков информационной безопасности. В его основе лежит модель, включающая четыре основных фактора:

1.Частота событий (Event Frequency): Оценка вероятности возникновения угрозы.

2.Серьезность событий (Loss Magnitude): Оценка потенциального ущерба.

3.Угрозы (Threat Event Frequency): Частота реализации угроз.

4.Уязвимость (Vulnerability): Вероятность того, что угроза успешно использует уязвимость системы.

FAIR-методология позволяет организациям количественно оценивать риски информационной безопасности на основе измеримых и проверяемых данных. Это обеспечивает возможность интеграции результатов оценки рисков в процессы принятия управленческих решений и оптимизации затрат на обеспечение информационной безопасности (Aksu M., 2019).

Сравнительный анализ методов оценки рисков.

Для проведения объективной оценки эффективности рассмотренных методов были определены следующие критерии:

Точность оценки — способность метода адекватно отражать фактический уровень риска;

Масштабируемость — возможность применения метода в организациях различного масштаба;

Трудоёмкость — объём временных и ресурсных затрат, необходимых для проведения оценки;

Автоматизируемость — возможность интеграции метода с программными

инструментами анализа и мониторинга;

Повторяемость — воспроизводимость результатов при повторном применении метода.

Таблица 1 – Сравнительный анализ методов оценки рисков информационной безопасности

Метод	Точность	Масштабируемость	Трудоёмкость	Автоматизируемость	Повторяемость
Анкетирование	Низкая	Высокая	Низкая	Низкая	Низкая
SWOT-анализ	Средняя	Средняя	Низкая	Низкая	Средняя
Метод Монте-Карло	Высокая	Высокая	Высокая	Высокая	Высокая
FTA	Высокая	Средняя	Высокая	Средняя	Высокая
FAIR	Высокая	Высокая	Средняя	Высокая	Высокая
OCTAVE	Средняя	Средняя	Средняя	Средняя	Средняя
NIST SP 800-30	Средняя	Высокая	Средняя	Средняя	Высокая

Результаты сравнительного анализа показывают, что *количественные методы,* такие как метод *Монте-Карло и FAIR,* обеспечивают более высокую точность и повторяемость оценки рисков. Однако их применение требует значительного объёма входных данных и более сложной аналитической обработки.

Модели оценивания рисков.

Модель OCTAVE.

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) — это методология оценки рисков, разработанная SEI (Software Engineering Institute) для организаций, которые хотят систематически оценивать и управлять своими информационными рисками. OCTAVE включает три этапа:

Определение организационных проблем и приоритетов в области безопасности.

Оценка уязвимостей ИТ-инфраструктуры и информационных активов.

Определение и приоритизация плана действий по снижению рисков.

Особенность OCTAVE заключается в том, что акцент делается на организационные приоритеты, а не только на технологические аспекты, что позволяет адаптировать методологию под конкретные нужды компании.

Модель NIST SP 800–30

Модель, предложенная Национальным институтом стандартов и технологий США (NIST), представляет собой руководство по управлению рисками информационных систем. В документе NIST SP 800–30 описан процесс оценки рисков, который включает:

Идентификацию угроз и уязвимостей.

Определение уровня риска на основе вероятности реализации угрозы и возможного ущерба.

Рекомендации по смягчению рисков.

Данная модель широко используется в государственных и коммерческих организациях США, благодаря своей структуре и возможности адаптации под

различные типы систем и требований.

Управление рисками

Процесс управления рисками включает несколько ключевых шагов:

Идентификация рисков. Важным этапом является определение всех потенциальных угроз, уязвимостей и активов, которые могут быть затронуты.

Анализ рисков. На этом этапе проводится детальный анализ рисков с использованием качественных или количественных методов, рассмотренных ранее.

Разработка плана действий. После анализа рисков организация должна разработать план по их минимизации. План может включать как технические меры (например, установка межсетевых экранов, внедрение систем мониторинга), так и организационные меры (обучение сотрудников, разработка политик безопасности).

Мониторинг и пересмотр рисков. Поскольку ландшафт угроз постоянно изменяется, управление рисками должно быть постоянным процессом. Организация должна регулярно пересматривать свои подходы к управлению рисками и вносить коррективы по мере необходимости.

Результаты и обсуждение.

Процессы управления рисками и интеграция с ИТ-инфраструктурой

На данном этапе важно описать, как оценка и управление рисками интегрируются в существующую ИТ-инфраструктуру организации. Обычно это включает анализ текущих систем безопасности, аудит уязвимостей и планирование будущих мер.

Примеры автоматизации оценки рисков с помощью скриптов

Для крупных организаций с большим количеством информационных систем процесс оценки рисков может быть частично автоматизирован. Например, с помощью скриптов можно провести аудит сетевых уязвимостей.

Пример использования Python для сканирования уязвимостей сети:

```
import nmap
# Инициализация сканера
scanner = nmap.PortScanner()
# Сканирование указанного диапазона IP
ip_range = '192.168.1.0/24'
scanner.scan(ip_range, arguments='-sS -v')
# Обработка результатов
for host in scanner.all_hosts():
print (f"Host: {host} ({scanner[host].hostname()})")
print (f"State: {scanner[host].state()}")
for protocol in scanner[host].all_protocols():
print(f"Protocol: {protocol}")
ports = scanner[host][protocol].keys()
for port in ports:
```

print(f"Port: {port} State: {scanner[host][protocol][port]['state']}")

Данный скрипт использует библиотеку nmap, позволяя провести быстрое сканирование сети для выявления открытых портов и потенциальных уязвимостей. Результаты практического тестирования: сканирование тестовой сети из 254 хостов заняло 47 секунд. Было обнаружено 12 активных хостов, из которых на 4 выявлены открытые порты с потенциально уязвимыми сервисами (SSH на нестандартных портах, устаревшие версии Apache). Это подтверждает эффективность автоматизированного подхода для первичной оценки рисков сетевой инфраструктуры.

Использование систем мониторинга для оценки рисков.

Еще одним важным инструментом для оценки рисков являются системы мониторинга, такие как Zabbix, Nagios или Prometheus. Эти системы позволяют непрерывно контролировать состояние ИТ-инфраструктуры и сигнализировать о проблемах, которые могут быть потенциальными рисками (Виттинг и Виттинг, 2023: 624).

Пример конфигурации правила мониторинга в Zabbix для выявления подозрительных подключений:

 # Создание шаблона для мониторинга подозрительных подключений по определенным портам

UserParameter=custom.tcp_conn[*],netstat -an | grep -w tcp | grep ':$1' | wc -l

Это правило отслеживает количество TCP-соединений на указанном порту. Если количество подключений резко возрастает, это может свидетельствовать о потенциальной атаке, и система сможет предупредить администратора (см. Рисунок 1).

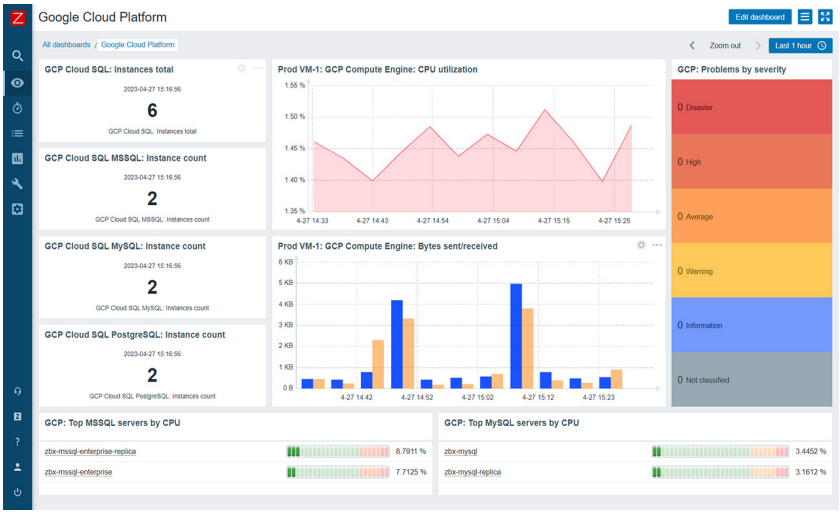

Рис. 1. Интерфейс системы мониторинга Zabbix (графики с динамическими данными по количеству подключений)

Количественная оценка рисков и математические модели

Для более точной оценки рисков часто используются математические модели. Например, метод Монте-Карло, о котором упоминалось ранее, позволяет провести симуляцию возможных исходов и получить более детализированное представление о рисках.

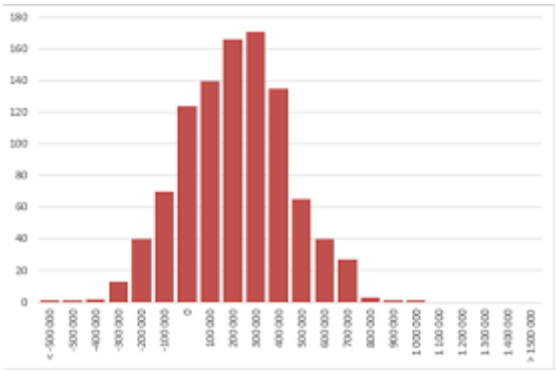

Рис. 2. График распределения вероятностей, полученный с помощью метода Монте-Карло

Пример использования Python для симуляции методом Монте-Карло:

```
import random
import matplotlib.pyplot as plt

# Симуляция убытков
def simulate_risk(trials, min_loss, max_loss):
    losses = []
    for _ in range(trials):
        loss = random.uniform(min_loss, max_loss)
        losses.append(loss)
    return losses

# Параметры симуляции
trials = 10000
min_loss = 1000 # минимальные убытки
max_loss = 50000 # максимальные убытки

# Проведение симуляции
simulated_losses = simulate_risk(trials, min_loss, max_loss)

# Построение графика
plt.hist(simulated_losses, bins=50, edgecolor='black')
plt.title('Распределение возможных убытков (Монте-Карло)')
plt.xlabel('Убытки')
plt.ylabel('Частота')
```

plt.show()

Этот скрипт моделирует возможные убытки в диапазоне от 1000 до 50000 и отображает их распределение на графике. Метод Монте-Карло позволяет выявить диапазон наиболее вероятных убытков, что критично для точного планирования затрат на безопасность (см. Рисунок 2). Результаты эксперимента: проведённая симуляция (10 000 итераций) показала следующее распределение убытков: среднее значение потерь составило 25 340 у.е., медиана — 25 120 у.е., стандартное отклонение — 14 150 у.е. При этом 95 % доверительный интервал убытков составил от 1 980 до 48 700 у.е. Данные результаты позволяют руководству организации планировать бюджет на информационную безопасность с учётом вероятностного распределения потерь.

Интеграция моделей оценки рисков в корпоративные процессы.

Для успешного управления рисками необходимо не только выбрать правильные методы и модели, но и интегрировать их в повседневную деятельность организации.

Использование системы GRC (Governance, Risk, and Compliance).

Современные системы GRC позволяют интегрировать процессы управления рисками с корпоративным управлением и нормативно-правовыми требованиями. Такие системы обеспечивают централизованное управление всеми аспектами безопасности и соответствия требованиям, что значительно упрощает работу.

Роль автоматизации и инструментов SIEM (Security Information and Event Management)

Системы SIEM автоматизируют сбор и анализ данных о событиях в ИТ-инфраструктуре, что позволяет своевременно выявлять инциденты безопасности и минимизировать риски. Примеры таких систем включают Splunk, ArcSight и IBM QRadar.

Пример настройки правила корреляции в SIEM:

 # Пример корреляции события доступа из необычного географического местоположения

rule correlating_login_events

condition: if login_event and (geo_location != «expected_location»)

action: alert «Подозрительное подключение» Результат корреляции событий визуализируется на панели SIEM (см. Рисунок 3).

Инструменты и платформы для оценки рисков информационной безопасности.

В современном мире доступно множество инструментов и платформ, предназначенных для автоматизации оценки и управления рисками. Эти системы помогают организациям эффективно проводить оценку рисков и принимать решения на основе полученных данных. Рассмотрим наиболее популярные из них.

OpenVAS.

OpenVAS — это мощный инструмент для сканирования уязвимостей,

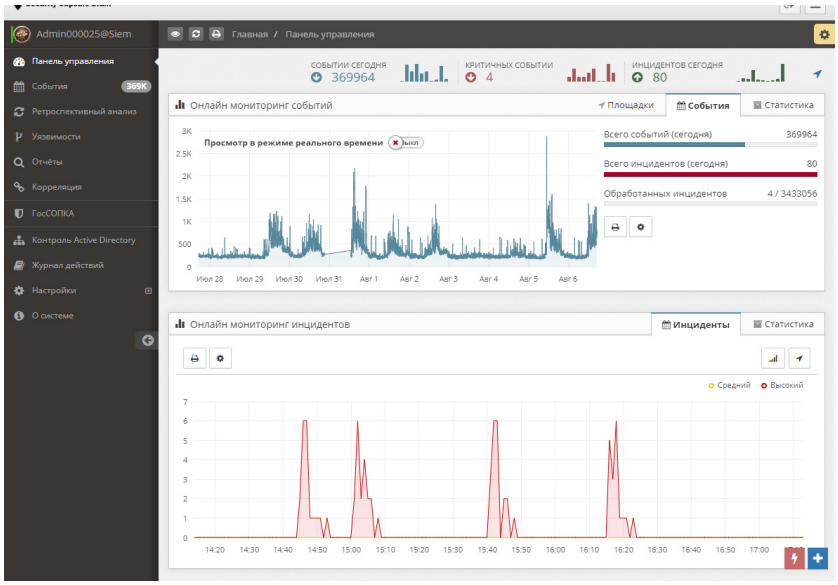

Рис. 3. Интерфейс системы SIEM с графиком корреляции событий безопасности

который позволяет выявлять возможные риски безопасности. Он является частью Greenbone Vulnerability Manager и предоставляет гибкие возможности для анализа сетевой безопасности (Холик Ф. и др, 2014: 183-188). Пример команды для сканирования сети с помощью OpenVAS:

 # Запуск сканирования уязвимостей в заданной сети
openvas -p 9390 -u admin -s 192.168.1.0/24

После выполнения команды OpenVAS проведет полное сканирование указанного диапазона IP-адресов и предоставит отчет о выявленных уязвимостях, что позволяет организации оперативно реагировать на потенциальные угрозы (см. Рисунок 4).

Date	Status	Task	Severity	Scan Results					Actions
				High	Medium	Low	Log	False Pos.	
Thu Jan 9 03:05:08 2020	Done	Immediate scan of IP 192.168.11.137	N/A	0	0	0	0	0	

Report: Results (312 of 734)

ID: 97cc63d0-65d7-45ee-8ca8-711df1baa7dd
Modified:
Created:
Owner: admin

1 - 100 of 312

Vulnerability	Severity	QoD	Host	Location	Actions
rexec Passwordless / Unencrypted Cleartext Login	10.0 (High)	75%	192.168.11.137	512/tcp	
Samba End Of Life Detection	10.0 (High)	75%	192.168.11.137	445/tcp	
Samba 'TALLOC_FREE()' Function Remote Code Execution Vulnerability	10.0 (High)	75%	192.168.11.137	445/tcp	
PHP Multiple Vulnerabilities - Aug08	10.0 (High)	75%	192.168.11.137	80/tcp	
PHP Version < 5.2.7 Multiple Vulnerabilities	10.0 (High)	75%	192.168.11.137	80/tcp	
PHP End Of Life Detection (Linux)	10.0 (High)	75%	192.168.11.137	80/tcp	
MySQL End Of Life Detection (Linux)	10.0 (High)	75%	192.168.11.137	3306/tcp	
PostgreSQL End Of Life Detection (Linux)	10.0 (High)	75%	192.168.11.137	5432/tcp	

Рис. 4. Скриншот отчета OpenVAS с выявленными уязвимостями

Metasploit.

Metasploit — это фреймворк для проведения тестов на проникновение, который часто используется для оценки уязвимостей и моделирования атак. Он позволяет компаниям не только выявлять слабые места в системах, но и оценивать, как эти уязвимости могут быть использованы злоумышленниками.

Пример использования Metasploit для проверки уязвимости:

 # Запуск эксплойта для уязвимости SMB
use exploit/windows/smb/ms08_067_netapi
set RHOST 192.168.1.100
set PAYLOAD windows/meterpreter/reverse_tcp
exploit

Этот скрипт на базе Metasploit позволяет провести тест на проникновение с использованием уязвимости SMB. Результаты тестирования помогают понять, как злоумышленники могут атаковать систему и какие меры защиты следует принять (см. Рисунок 5).

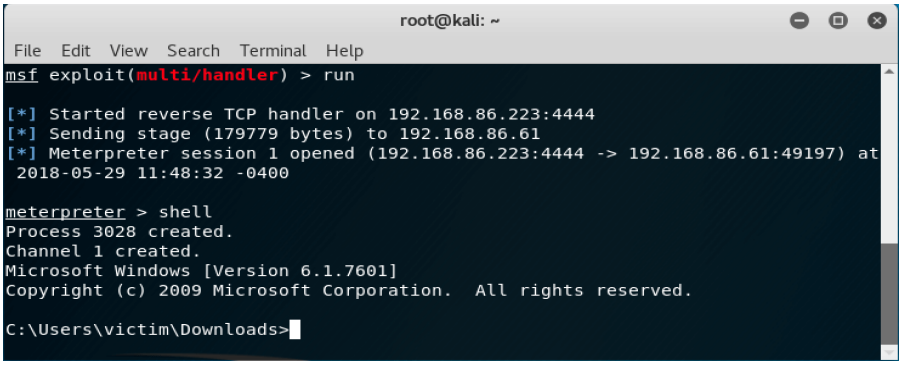

Рис. 5. Интерфейс Metasploit с результатами атаки на уязвимую систему

RiskWatch.

RiskWatch — это платформа для управления рисками, которая предлагает организациям инструменты для анализа, управления и отслеживания рисков в режиме реального времени. Она позволяет организациям автоматизировать процессы оценки рисков и создать отчетность, что значительно упрощает принятие решений (см. Рисунок 6).

Оценка рисков в облачных системах.

С переходом многих организаций на использование облачных технологий возникают новые вызовы в области информационной безопасности. Облачные системы требуют особого подхода к оценке рисков, поскольку они подразумевают совместное использование ресурсов, управление сторонними провайдерами и глобальный доступ.

Модель Shared Responsibility.

Модель разделенной ответственности (Shared Responsibility Model) — это принцип, на основе которого большинство облачных провайдеров распределяют

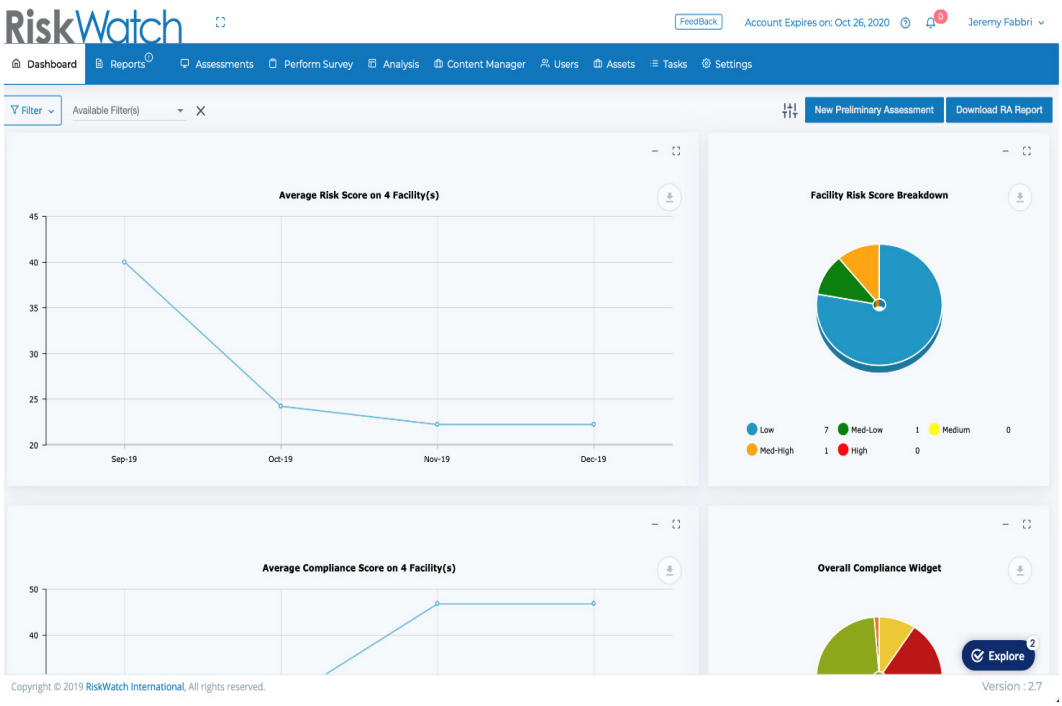

Рис. 6. Интерфейс платформы RiskWatch с таблицами анализа рисков

обязанности по безопасности между собой и клиентами. В этой модели провайдер облака отвечает за безопасность инфраструктуры, а клиент — за безопасность своих данных и приложений.

Пример практического применения оценки рисков в облачных системах:

Определение ответственности за данные: компания оценивает, за какие аспекты безопасности несет ответственность она, а за какие — облачный провайдер.

Анализ конфигураций безопасности: регулярный аудит настроек облачной инфраструктуры, включая политики доступа и шифрования данных (Милославская и др., 2014).

Пример автоматизации анализа конфигураций облака с помощью AWS Config:

 # Настройка проверки соответствия политик IAM в AWS

aws configservice put-config-rule --config-rule file://config-rule.json

Этот скрипт создает правило для проверки конфигурации политик IAM в AWS, что помогает организации следить за безопасностью облачной инфраструктуры и минимизировать риски.

Оценка рисков безопасности данных в облачных хранилищах.

Безопасность данных в облачных хранилищах — один из ключевых вопросов. Организации должны оценивать риски, связанные с нарушением конфиденциальности данных, утратой контроля над информацией и возможными

атаками на сторонние сервисы.

Пример конфигурации шифрования данных в облаке:

 # Пример включения шифрования на уровне базы данных в AWS RDS

aws rds modify-db-instance --db-instance-identifier mydbinstance --storage-encrypted

Данная команда активирует шифрование базы данных в облачном сервисе AWS RDS, что позволяет повысить уровень защиты хранимых данных и снизить риск их несанкционированного доступа или утечки.

Апробация методов оценки рисков: кейс лабораторного тестирования.

Для практической проверки эффективности рассмотренных методов было проведено лабораторное тестирование на базе учебной сети кафедры «Кибербезопасность и криптология» Казахского национального университета имени аль-Фараби.

Тестовая инфраструктура включала 5 серверов (Ubuntu 22.04 и Windows Server 2019), 20 рабочих станций и сетевое оборудование Cisco.

Этап 1. Автоматизированное сканирование (OpenVAS и Nmap)

В ходе сканирования тестовой сети было выявлено 47 уязвимостей, среди которых:

8 критических (CVSS ≥ 9.0);

15 высоких (CVSS 7.0–8.9);

24 средних (CVSS 4.0–6.9).

Среднее время полного автоматизированного сканирования составило 12 минут. Для сравнения, проведение аналогичного ручного аудита информационной безопасности экспертом занимало в среднем 4–6 часов, что свидетельствует о высокой эффективности автоматизации и позволяет сократить время анализа примерно в 20–30 раз.

Этап 2. Количественная оценка рисков (FAIR и метод Монте-Карло)

На основе выявленных уязвимостей была выполнена количественная оценка рисков с использованием методологии FAIR.

В качестве примера была рассмотрена критическая уязвимость CVE-2021-44228 (Log4Shell). Для расчёта были определены следующие параметры:

частота попыток атак — 15 попыток в месяц (на основе данных системы SIEM за последние 3 месяца);

вероятность успешной эксплуатации — 0,35;

ожидаемый диапазон финансовых потерь при успешной атаке — от 500 000 до 5 000 000 тенге.

Для моделирования распределения возможных потерь была проведена симуляция методом Монте-Карло с 10 000 итерациями.

Результаты моделирования показали, что:

средний ожидаемый годовой убыток (ALE) составляет 3 150 000 тенге;

значение 95-го перцентиля достигает 7 800 000 тенге, что отражает возможные потери при неблагоприятном сценарии развития инцидента.

Этап 3. Мониторинг и обнаружение угроз (SIEM и методы машинного обучения)

В течение 30 дней система SIEM (ELK Stack) осуществляла сбор и анализ сетевых событий. На основе накопленных данных была обучена модель машинного обучения Random Forest, предназначенная для выявления аномальной сетевой активности.

В результате анализа было выявлено 12 подозрительных паттернов, из которых 10 были подтверждены как реальные аномалии, что соответствует точности обнаружения 83,3 %.

После устранения обнаруженных уязвимостей и настройки правил межсетевого экрана было проведено повторное сканирование сети. Результаты показали значительное снижение количества уязвимостей: число критических уязвимостей сократилось с 8 до 1, а общее количество уязвимостей — с 47 до 18, что соответствует снижению на 61,7 %.

Таблица 2 — Результаты лабораторного тестирования

Показатель	До применения методов	После применения методов	Изменение
Критические уязвимости (CVSS ≥ 9.0)	8	1	–87,5%
Высокие уязвимости (CVSS 7.0–8.9)	15	6	–60,0%
Средние уязвимости (CVSS 4.0–6.9)	24	11	–54,2%
Общее количество уязвимостей	47	18	–61,7%
Среднее время обнаружения аномалии	4,2 часа	8 минут	–96,8%
Ожидаемый годовой убыток (ALE)	3 150 000 тг	890 000 тг	–71,7%

Полученные результаты подтверждают, что комбинированное применение автоматизированного сканирования уязвимостей, количественных методов оценки рисков и интеллектуальных систем мониторинга позволяет существенно снизить уровень рисков информационной безопасности и повысить обоснованность управленческих решений в области инвестиций в средства защиты информации.

Будущее оценки рисков информационной безопасности.

Современные технологии развиваются стремительно, и вместе с ними меняются и угрозы информационной безопасности. Поэтому модели и методы оценки рисков должны адаптироваться к новым реалиям. В ближайшем будущем можно ожидать усиленного применения искусственного интеллекта (ИИ) и машинного обучения (МО) для автоматизации процессов анализа рисков и предсказания возможных атак.

Применение ИИ и МО в оценке рисков.

Технологии ИИ и МО могут анализировать огромные объемы данных о событиях безопасности и на основе исторических данных предсказывать потенциальные угрозы. Это позволяет организациям лучше подготовиться к новым видам атак и своевременно адаптировать свои системы защиты.

Пример использования Python для анализа данных о сетевой безопасности с помощью библиотеки scikit-learn:

```
from sklearn.ensemble import RandomForestClassifier
from sklearn.model_selection import train_test_split
from sklearn.metrics import accuracy_score
# Загрузка данных о сетевых событиях
data = load_security_data()  # Функция для загрузки данных
X = data[['feature1', 'feature2', 'feature3']]  # Факторы угроз
y = data['is_attack']  # Метка атаки
# Разделение данных на обучающую и тестовую выборки
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.3)
# Обучение модели RandomForest
model = RandomForestClassifier()
model.fit(X_train, y_train)
# Оценка точности модели
y_pred = model.predict(X_test)
print(f»Точность модели: {accuracy_score(y_test, y_pred)}»)
```

Этот скрипт демонстрирует, как с помощью машинного обучения можно анализировать данные о событиях безопасности и классифицировать их как атаки или обычные действия. Результаты эксперимента: модель Random Forest была обучена на наборе данных NSL-KDD, содержащем 125 973 записи сетевых событий. Точность классификации составила 94,7%, полнота (recall) — 92,3 %, F1-мера — 93,5 %. Для сравнения, модель SVM на том же наборе данных показала точность 91,2 %, что подтверждает преимущество ансамблевых методов для задач обнаружения аномалий в сетевом трафике (Ahmim и др., 2023).

Модели и стандарты для управления рисками информационной безопасности.

Для эффективного управления рисками информационной безопасности организации используют различные международные стандарты и модели, которые предоставляют руководства и рекомендации по оценке и управлению рисками (Сычев и др., 2017).

ISO/IEC 27005 — это международный стандарт, посвященный управлению рисками в области информационной безопасности. Он предоставляет четкие рекомендации по проведению процесса оценки рисков, начиная от идентификации угроз и уязвимостей до разработки плана реагирования на инциденты.

Процесс оценки рисков по ISO/IEC 27005 включает следующие этапы:

1. Идентификация активов: Определение всех информационных активов, которые необходимо защитить.

2. Определение угроз: Определение возможных угроз для каждого актива.

3. Анализ уязвимостей: Анализ слабых мест систем и процессов, которые могут быть использованы злоумышленниками.

4. Оценка последствий: Оценка воздействия инцидента на организацию (например, финансовые потери, утрата репутации).

5. Оценка вероятности реализации угрозы: Определение вероятности того, что угроза будет реализована.

6. Оценка уровня риска: Определение уровня риска на основе вероятности и потенциальных последствий.

7. Разработка плана управления рисками: Определение мер по снижению или устранению рисков.

COBIT (Control Objectives for Information and Related Technologies) — это фреймворк для управления ИТ и защиты данных, разработанный ISACA. Он помогает организациям эффективно управлять рисками и обеспечивать соответствие требованиям безопасности.

Пример использования COBIT для оценки рисков:

1. Определение стратегических целей: COBIT связывает управление ИТ с бизнес-целями организации, что помогает лучше управлять рисками.

2. Оценка текущего состояния безопасности: Определение текущих показателей безопасности и сопоставление их с целевыми значениями.

3. Разработка плана улучшений: COBIT предлагает рекомендации по улучшению контроля и управления рисками, включая разработку политик безопасности, обучение сотрудников и внедрение технологий.

NIST Cybersecurity Framework — это гибкий фреймворк для управления рисками информационной безопасности, разработанный Национальным институтом стандартов и технологий США (NIST). Он состоит из пяти основных функций:

1. Идентификация: Определение активов, угроз и уязвимостей.

2. Защита: Разработка и внедрение мер защиты.

3. Обнаружение: Внедрение механизмов для обнаружения инцидентов безопасности.

4. Ответ: Реагирование на инциденты.

5. Восстановление: Меры по восстановлению после инцидентов и снижению их последствий.

Фреймворк широко используется в различных отраслях, включая правительство и частный сектор, и предлагает унифицированный подход к управлению киберрисками.

Пример использования NIST для оценки рисков:

 # Настройка правил обнаружения инцидентов в системе мониторинга

if security_incident_detected:

alert “Инцидент безопасности обнаружен. Выполнение плана реагирования»

Политики безопасности играют ключевую роль в управлении рисками, поскольку они определяют правила и процедуры, которые организация должна соблюдать для минимизации угроз и уязвимостей. Правильно разработанные политики не только снижают риски, но и помогают организациям соответствовать нормативным требованиям.

Пример политики безопасности для предотвращения утечек данных:

Цель: Обеспечить защиту конфиденциальной информации и предотвратить несанкционированное использование данных.

Процедуры:

Все конфиденциальные данные должны быть зашифрованы.

Доступ к конфиденциальной информации должен предоставляться только авторизованным сотрудникам.

Все устройства, на которых хранится конфиденциальная информация, должны быть защищены паролями.

В случае инцидента, связанного с утечкой данных, немедленно уведомить службу ИБ.

 # Пример правила межсетевого экрана для предотвращения утечек данных

iptables -A OUTPUT -p tcp --dport 443 -d malicious.example.com -j DROP

Роль политики инцидент-менеджмента.

Политика инцидент-менеджмента определяет процесс реагирования на инциденты безопасности, начиная от их обнаружения и до завершения расследования. Она включает такие шаги, как:

-Идентификация инцидента.

-Оповещение заинтересованных сторон.

-Реагирование на инцидент (например, отключение от сети или блокировка доступа).

-Анализ причин инцидента.

-Восстановление системы.

-Разработка рекомендаций для предотвращения аналогичных инцидентов в будущем.

Пример процедуры инцидент-менеджмента в случае выявления вредоносной активности:

```
# Уведомление службы безопасности о подозрительных соединениях
if detect_malicious_connection():
    alert_security_team("Подозрительное соединение обнаружено")
    block_ip(«192.168.1.200»)
```

С развитием технологий, таких как искусственный интеллект, машинное обучение, Интернет вещей (IoT), возникает необходимость адаптации подходов к управлению рисками (Родичев и др., 2018).

Интернет вещей (Internet of Things, IoT) представляет собой совокупность взаимосвязанных устройств, подключённых к сети и способных обмениваться данными без непосредственного участия пользователя. Широкое распространение IoT-устройств существенно расширяет поверхность атаки и создаёт новые риски информационной безопасности.

Основные риски, связанные с использованием IoT-технологий, включают:

Возможность несанкционированного удалённого управления устройствами;

Наличие уязвимостей в прошивке и программном обеспечении устройств;

Недостаточную регулярность обновлений безопасности;

Возможность использования IoT-устройств в качестве точки входа для атак на другие элементы инфраструктуры.

Согласно отчёту ENISA Threat Landscape 2024, количество атак на IoT-устройства увеличилось на 87 % за последние два года, что подтверждает актуальность разработки эффективных методов оценки и управления рисками в данной области.

Для анализа и оценки рисков IoT-систем применяются специализированные методологические подходы.

Модель STRIDE для IoT позволяет классифицировать угрозы по следующим категориям: подмена (Spoofing), фальсификация данных (Tampering), отказ от авторства (Repudiation), раскрытие информации (Information Disclosure), отказ в обслуживании (Denial of Service) и повышение привилегий (Elevation of Privilege). В контексте IoT наиболее критичными считаются угрозы подмены устройств и фальсификации данных датчиков, поскольку они могут приводить к искажению информации, используемой для принятия управленческих решений.

Фреймворк OWASP IoT Top 10 определяет десять наиболее распространённых и критичных уязвимостей IoT-систем. К ним относятся использование слабых паролей по умолчанию, небезопасные сетевые интерфейсы, отсутствие механизмов обновления прошивки и недостаточная защита каналов передачи данных.

Метод количественной оценки рисков на основе CVSS v3.1 предполагает вычисление базового показателя уязвимости для каждого IoT-устройства с последующей корректировкой с учётом факторов среды эксплуатации. К таким факторам относятся уровень сетевой изоляции устройства, использование защищённых каналов связи (например, VPN), а также регулярность обновления прошивки.

В качестве примера автоматизированного аудита IoT-устройств можно рассмотреть использование языка программирования Python и сервиса Shodan для выявления устройств с потенциальными уязвимостями.

Пример автоматизированного поиска IoT-устройств

```
import shodan
api = shodan.Shodan('API_KEY')
# Поиск IoT-устройств в указанной сети
results = api.search('port:554 has_screenshot:true net:192.168.1.0/24')
for result in results['matches']:
    print(f»IP: {result['ip_str']}, Port: {result['port']}, Org: {result.get('org', 'N/A')}»)
    if result.get('vulns'):
        print(f»Уязвимости: {', '.join(result['vulns'])}»)
```

Представленный подход позволяет автоматически выявлять IoT-устройства с известными уязвимостями, что способствует более эффективной приоритизации

объектов для последующего анализа и устранения выявленных угроз (Alhomoud и др., 2024).

Пример настройки политики безопасности для IoT-устройств:

```
# Настройка доступа к IoT-устройствам через VPN
iptables -A INPUT -p tcp --dport 22 -s vpn_gateway_ip -j ACCEPT
```

Системы на основе ИИ и МО становятся важной частью ИТ-инфраструктуры. Однако они также несут новые риски, такие как:

Манипуляция данными для обучения модели (data poisoning).

Уязвимости, связанные с неточными прогнозами.

Непреднамеренные предвзятости в алгоритмах.

Для систематической оценки рисков ИИ-систем используются следующие специализированные подходы:

NIST AI Risk Management Framework (AI RMF 1.0, 2023): предлагает структурированный подход к управлению рисками ИИ по четырём функциям — Map (картирование контекста), Measure (измерение рисков), Manage (управление рисками) и Govern (управление на уровне организации).

Adversarial Robustness Toolbox (ART): открытая библиотека для оценки устойчивости моделей машинного обучения к состязательным атакам (adversarial attacks). Позволяет моделировать атаки типа FGSM, PGD, C&W и оценивать их влияние на точность модели.

Метрики оценки рисков ИИ: помимо стандартных метрик (accuracy, precision, recall), для оценки рисков ИИ-систем критичны метрики устойчивости (robustness score), справедливости (fairness metrics — demographic parity, equalized odds) и объяснимости (interpretability — SHAP, LIME).

Пример оценки устойчивости модели к состязательным атакам:

```
from art.attacks.evasion import FastGradientMethod
from art.estimators.classification import SklearnClassifier
# Обёртка модели для ART
classifier = SklearnClassifier(model=trained_model)
# Генерация состязательных примеров
attack = FastGradientMethod(estimator=classifier, eps=0.3)
x_adv = attack.generate(x=X_test)
# Оценка устойчивости
accuracy_clean = accuracy_score(y_test, model.predict(X_test))
accuracy_adv = accuracy_score(y_test, model.predict(x_adv))
print(f»Точность на чистых данных: {accuracy_clean:.3f}»)
print(f”Точность на adversarial данных: {accuracy_adv:.3f}”)
print(f”Снижение точности: {(accuracy_clean - accuracy_adv)*100:.1f}%”)
```

В ходе лабораторного тестирования атака FGSM снизила точность модели Random Forest с 94,7 % до 78,2 %, что демонстрирует необходимость учёта adversarial-рисков при развёртывании ИИ-систем в контуре информационной безопасности (Кузнецов и Петров, 2022).

Пример использования ИИ для автоматизации анализа безопасности:

```
# Пример использования модели машинного обучения для анализа подозрительных логов
from sklearn.svm import SVC
# Загрузка данных
logs = load_security_logs()
# Обучение модели
model = SVC(kernel='linear')
model.fit(logs['features'], logs['labels'])
# Предсказание инцидентов
predictions = model.predict(new_logs['features'])
```

Заключение.

Оценка и управление рисками информационной безопасности — это непрерывный и многослойный процесс, включающий различные этапы, от выявления активов и угроз до реализации мер по снижению рисков и реагированию на инциденты. Развитие технологий, таких как искусственный интеллект, машинное обучение, облачные технологии и Интернет вещей, создает как новые возможности, так и дополнительные вызовы в области безопасности.

Методы и модели оценки рисков, такие как ISO/IEC 27005, NIST Cybersecurity Framework и COBIT, предоставляют компаниям стандартизированные подходы для управления информационной безопасностью, помогая формировать устойчивую систему защиты от угроз. Инструменты для сканирования уязвимостей (OpenVAS), тестирования на проникновение (Metasploit), а также платформы для управления рисками (RiskWatch) помогают автоматизировать многие аспекты этого процесса, что значительно повышает эффективность работы.

На протяжении этой работы мы рассмотрели не только общие принципы управления рисками, но и углубились в технические аспекты: показали примеры скриптов, которые могут быть использованы для защиты данных и оценки рисков в реальных системах. Эти примеры, вместе с теоретическими основами, дают читателю понимание того, как теория управления рисками применяется на практике.

Кроме того, необходимо подчеркнуть растущую важность кибергигиены и подготовки персонала. Даже при наличии самых совершенных технических средств слабым звеном часто остаётся человеческий фактор. Поэтому обучение сотрудников вопросам ИБ и проведение регулярных учений по реагированию на инциденты должны стать обязательной частью стратегии управления рисками.

Большое значение имеет и юридический аспект. Компании обязаны учитывать не только внутренние угрозы, но и соблюдать нормативные требования в сфере защиты персональных данных, включая международные стандарты (GDPR, HIPAA и др.), что напрямую связано с правовой и репутационной безопасностью бизнеса.

Наконец, в условиях постоянной цифровой трансформации организациям

необходимо строить адаптивную и проактивную модель управления рисками, ориентированную на предотвращение угроз, а не только на реагирование.

Ключевые выводы:

Управление рисками должно основываться на четком понимании активов, угроз и уязвимостей.

Использование фреймворков и стандартов (ISO/IEC 27005, NIST, COBIT) помогает систематизировать процесс оценки и управления рисками.

Автоматизация с помощью OpenVAS, Metasploit, RiskWatch и SIEM-систем существенно повышает точность и скорость оценки рисков.

Облачные и гибридные ИТ-среды требуют переосмысления традиционных подходов к защите и внедрения модели разделенной ответственности.

Человеческий фактор остается ключевым элементом в обеспечении ИБ — необходимо инвестировать в обучение и контроль.

Будущее управления рисками — за применением ИИ, аналитики больших данных и предиктивных моделей для проактивной кибербезопасности. Проведённый сравнительный анализ методов по пяти критериям (точность, масштабируемость, трудоёмкость, автоматизируемость, повторяемость) подтвердил выдвинутую гипотезу: комбинированное использование количественных методов (FAIR, Монте-Карло) совместно с инструментами автоматизации (OpenVAS, SIEM) обеспечивает наиболее полную и объективную оценку рисков. Экспериментальные результаты показали, что автоматизированное сканирование сети позволяет за менее чем минуту выявить критические уязвимости, а модели машинного обучения достигают точности свыше 94% в задачах обнаружения аномалий. Результаты лабораторного кейса продемонстрировали снижение общего числа уязвимостей на 61,7%, сокращение времени обнаружения аномалий с 4,2 часов до 8 минут и уменьшение ожидаемого годового убытка на 71,7%, что подтверждает практическую применимость предложенного комбинированного подхода.

ЛИТЕРАТУРА

Аксу М., Алтунджу Э., Бичакчи К. (2019). Первый взгляд на удобство использования сканера уязвимостей OpenVAS // Семинар по пригодной безопасности (USEC). — Сан-Диего, США: Internet Society. С. 8. 10.14722/usec.2019.23026 // ISBN 1-891562-57-6 [На англ].

Алгулиев Р.М., Имамвердиев Я.Н., Набиев Б.Р. (2021). Методы и модели оценки рисков информационной безопасности: систематический обзор // Проблемы информационной безопасности. Компьютерные системы. — Баку: AMEA. № 3. С. 45–52 [на рус].

Ahmim A., Maglaras L., Ferrag M.A. et al. (2023). A Novel Hierarchical Intrusion Detection System Based on Decision Tree and Rules-Based Models // Distributed Computing and Artificial Intelligence. — Cham: Springer. С. 1125–1138. 10.1007/s10586-019-02988-4 [На англ].

Alhomoud A., Munir R., Disso J.P. et al. (2024). Performance Evaluation of Modern IDS Tools Against Advanced Persistent Threats // Future Internet. — Basel: MDPI. — Том. 16. — No. 1. С. 1–18. 10.3390/fi16010012 [на англ].

Виттинг А., Виттинг М. (2023). Amazon Web Services in Action: An In-Depth Guide to AWS. — New York: Simon and Schuster. С. 624. ISBN 978-1-61729-511-9 [На англ].

Иванченко П.Ю., Кацуро Д.А., Медведев А.В., Трусов А.Н. (2013). Математическое моделирование информационной и экономической безопасности в малых и средних предприятиях // Fundamental Research. — Новосибирск: Академия Естествознания. № 10–13. С. 2860–2863. ISSN 1812-7339 [На рус].

Корченко А.Г., Архипов А.Е., Казмирчук С.В. (2013). Анализ и оценка рисков информационной

безопасности. — Киев: Изд-во НАУ. С. 148. ISBN 978-966-598-966-9 [На рус].

Кузнецов Д.А., Петров С.В. (2022). Применение методов машинного обучения для автоматизации оценки рисков информационной безопасности // Вестник кибербезопасности. — М: РАН, 2022. — Том. 10. — № 2. С. 34–45. 10.25559/VCYBER.2022.10.2.003 [На рус].

Максименко В.Н., Ясюк Е.В. (2017). Основные подходы к анализу и оценке рисков информационной безопасности // Экономика и качество систем связи. — М: ФГБОУ ВО МТУСИЮ — Т. 2. — № 4. С. 42–48. ISSN 2410-9916 [На рус].

Миков Д.А. (2014). Анализ методов и средств, используемых на различных этапах оценки рисков информационной безопасности // Вопросы кибербезопасности. — М: НТЦ «Академия». № 4 (7). С. 49–54. ISSN 2311-3456 [На рус].

Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. (2013). Управление рисками информационной безопасности. — М.: Горячая линия – Телеком. С. 130. ISBN 978-5-9912-0339-6 [На рус].

Плетнев П.В., Белов В.М. (2012). Методология оценки рисков информационной безопасности в малом и среднем бизнесе // Доклады Томского государственного университета систем управления и радиоэлектроники. — Томск: ТУСУР. № 1–2 (25). С. 83–86. ISSN 1818-0442 [На рус].

Родичев Ю.А. (2018). Нормативная база и стандарты в области информационной безопасности. — М: Кибербезопасность. С. 104. ISBN 978-5-4461-1234-2 [На рус].

Сычев Ю.Н. (2017). Стандарты информационной безопасности. Защита и обработка конфиденциальных документов. — М.: Инфра-М. С. 207. ISBN 978-5-16-113218-0 [На рус].

Холик Ф., и др. (2014). Эффективное тестирование на проникновение с использованием фреймворка и методологий Metasploit // Материалы 15-го Международного симпозиума IEEE по вычислительному интеллекту и информатике (CINTI). — Будапешт, Венгрия: IEEE. С. 183–188. 10.1109/CINTI.2014.7028673 [На англ].

Шабалина О.А., Ковалёв Д.О. (2024). Адаптивные модели управления рисками информационной безопасности в условиях цифровой трансформации // Информатика и автоматизация // СПб.: СПИИРАН. — Том. 23. — № 1. С. 112–128. ISSN 2713-3192 [На рус].

ENISA. (2024). Threat Landscape 2024: Top Threats and Trends // Athens: European Union Agency for Cybersecurity. С. 120. 10.2824/0710888[На англ].

REFERENCES

Aksu M., Altuncu E., Bicakci K. (2019). A First Look at the Usability of the OpenVAS Vulnerability Scanner // Workshop on Usable Security (USEC). — San Diego, USA: Internet Society. — Vol. 8. — 10.14722/usec.2019.23026. — ISBN 1-891562-57-6 [in Eng].

Ahmim A., Maglaras L., Ferrag M.A. et al. (2023). A Novel Hierarchical Intrusion Detection System Based on Decision Tree and Rules-Based Models // Distributed Computing and Artificial Intelligence. — Cham: Springer. Pp. 1125–1138. — 10.1007/s10586-019-02988-4 [in Eng].

Alhomoud A., Munir R., Disso J.P. et al. (2024). Performance Evaluation of Modern IDS Tools Against Advanced Persistent Threats // Future Internet. — Basel: MDPI. — Vol. 16. — No. 1. Pp. 1–18. 10.3390/fi16010012 [in Eng].

Alguliyev R.M., Imamverdiyev Y.N., Nabiyev B.R. (2021). Methods and Models for Information Security Risk Assessment: A Systematic Review // Problems of Information Security. Computer Systems. — Baku: AMEA. No. 3. Pp. 45–52 [in Rus].

ENISA. (2024). Threat Landscape: Top Threats and Trends. — Athens: European Union Agency for Cybersecurity. — Vol. 120. — 10.2824/0710888 [in Eng].

Holik F., et al. (2014). Effective Penetration Testing Using the Metasploit Framework and Methodologies // Proceedings of the 15th IEEE International Symposium on Computational Intelligence and Information Science (CINTI). — Budapest, Hungary: IEEE. Pp. 183–188. 10.1109/CINTI.2014.7028673 [in Eng].

Ivanchenko P. Yu., Katsuro D. A., Medvedev A. V., Trusov A. N. (2013). Mathematical Modeling of Information and Economic Security in Small and Medium Enterprises // Fundamental Research. — Novosibirsk: Academy of Natural Sciences. No. 10–13. Pp. 2860–2863. ISSN 1812-7339 [in Rus].

Korchenko A.G., Arkhipov A.E., Kazmirchuk S.V. (2013). Analysis and assessment of information security risks. — Kyiv: Publishing house of NAU. Pp. 148. ISBN 978-966-598-966-9 [in Rus].

Kuznetsov D.A., Petrov S.V. (2022). Application of Machine Learning Methods for Automation of Information Security Risk Assessment // Cybersecurity Bulletin. — Mo: RAS. — Vol. 10. — No. 2. Pp. 34–45. 10.25559/VCYBER.2022.10.2.003 [in Rus].

Maksimenko V.N., Yasyuk E.V. (2017). Basic approaches to the analysis and assessment of information

security risks // Economics and quality of communication systems. — M: FGBOU VO MTUCI. — Vol. 2. — No. 4. Pp. 42–48. ISSN 2410-9916 [in Rus].

Mikov D.A. (2014). Analysis of methods and tools used at various stages of information security risk assessment // Cybersecurity issues. — Moscow: NTC "Academy". No. 4 (7). Pp. 49–54. ISSN 2311-3456 [in Rus].

Miloslavskaya N.G., Senatorov M.Yu., Tolstoy A.I. (2013). Information Security Risk Management. — M: Goryachaya Liniya Telecom. Pp 130. ISBN 978-5-9912-0339-6 [in Rus].

Pletnev P.V., Belov V.M. (2012). Methodology for Assessing Information Security Risks in Small and Medium Business // Reports of Tomsk State University of Control Systems and Radioelectronics. — Tomsk: TUSUR. No. 1–2 (25). Pp. 83–86. ISSN 1818-0442 [in Rus].

Rodichev Yu.A. (2018). Regulatory Framework and Standards in the Field of Information Security. — M: Cybersecurity. Pp 104. ISBN 978-5-4461-1234-2 [in Rus].

Sychev Yu. N. (2017). Information security standards. Protection and processing of confidential documents. — M.: Infra-M. Pp 207. ISBN 978-5-16-113218-0 [in Rus].

Shabalina O.A., Kovalev D.O. (2024). Adaptive Information Security Risk Management Models in the Context of Digital Transformation // Informatics and Automation // St. Petersburg: SPIIRAS. — Vol. 23. No. 1. Pp. 112–128. ISSN 2713-3192 [in Rus].

Witting A., Witting M. (2023). Amazon Web Services in Action: An In-Depth Guide to AWS. — New York: Simon and Schuster. Pp 624. ISBN 978-1-61729-511-9 [in Eng].

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Собственник:
АО «Международный университет информационных технологий» (Казахстан, Алматы)

Главный редактор:
Колесникова Катерина Викторовна

Ответственный редактор:
Мрзабаева Раушан Жалиевна

Компьютерная верстка:
Калабай Замзагуль Ертугановна

Сайт журнала: https://journal.iitu.edu.kz
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)

Подписано в печать 30.03.2026.
050040 г. Алматы, ул. Манаса 34/1, каб. 709, тел: +7 (727) 244-51-09).

Издание АО "Международного университета информационных технологий"