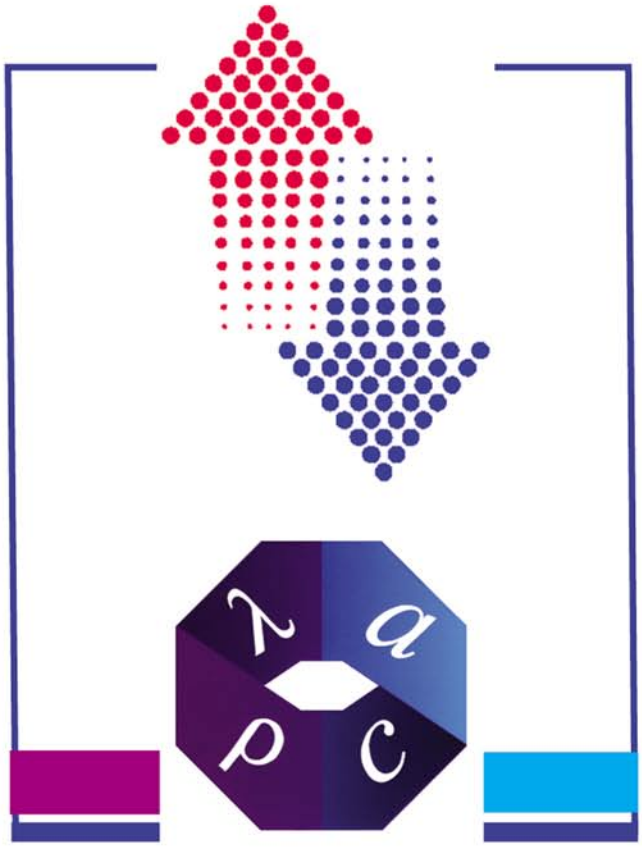
ИТМО

МАТЕРИАЛЫ МЕЖДУНАРОДНЫХ НАУЧНО-ТЕХНИЧЕСКИХ КОНФЕРЕНЦИЙ



СОВРЕМЕННЫЕ МЕТОД Ы И СРЕДСТВА ИССЛЕДОВАНИЙ ТЕПЛОФИЗИЧЕСКИХ СВОЙСТВ ВЕЩЕСТВ

(25–26 мая 2023 год)

ИСКУССТВЕННЫЙ ХОЛОД В XXI ВЕКЕ

(15–17 ноября 2023 год)

Санкт-Петербург
2024

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

ЭНЕРГОЭФФЕКТИВНЫЕ ИНЖЕНЕРНЫЕ СИСТЕМЫ

Материалы международных научно-технических конференций

«Современные методы и средства исследований теплофизических свойств веществ»

(25-26 мая 2023 год)

«Искусственный холод в XXI веке»

(15-17 ноября 2023 год)

Сборник научных трудов

Санкт-Петербург
2024

УДК 004, 063, 065, 504
ББК 20, 32, 40

Энергоэффективные инженерные системы. Материалы международных научно-технических конференций. «Современные методы и средства исследований теплофизических свойств веществ» (25-26 мая 2023 год). «Искусственный холод в XXI веке» (15-17 ноября 2023 год). Сборник научных трудов. – СПб.: Университет ИТМО, 2024. 404 с.

Издание содержит тезисы докладов, представленные на Международных научно-технических конференциях: «Современные методы и средства исследований теплофизических свойств веществ», «Искусственный холод в XXI веке», организованных Образовательным центром «Энергоэффективные инженерные системы» в 2023 году. В сборнике представлены доклады по следующим научным направлениям: актуальные вопросы реализации низкотемпературных, пищевых и эко- технологий в регионах России и в мире, современные методы и средства исследований теплофизических свойств веществ, промышленный холод и энергоэффективные низкотемпературные системы, криогенная техника, водородные технологии и технологии СПГ, системы жизнеобеспечения, пищевые системы и консервирование холодом, экономическая и экологическая эффективность предприятий.

Под редакцией доктора технических наук, профессора И.В. Баранова.

ISBN 978-5-7577-0707-5

ИТМО (Санкт-Петербург) – национальный исследовательский университет, научно-образовательная корпорация. Альма-матер победителей международных соревнований по программированию. Приоритетные направления: IT и искусственный интеллект, фотоника, робототехника, квантовые коммуникации, трансляционная медицина, Life Sciences, Art&Science, Science Communication.
Лидер федеральной программы «**Приоритет-2030**», в рамках которой реализовывается программа «Университет открытого кода». С 2022 ИТМО работает в рамках новой модели развития — научно-образовательной корпорации. В ее основе академическая свобода, поддержка начинаний студентов и сотрудников, распределенная система управления, приверженность открытому коду, бизнес-подходы к организации работы. Образование в университете основано на выборе индивидуальной траектории для каждого студента.
ИТМО пять лет подряд – в сотне лучших в области Automation & Control (кибернетика) Шанхайского рейтинга. По версии SuperJob занимает первое место в Петербурге и второе в России по уровню зарплат выпускников в сфере IT. Университет в топе международных рейтингов среди российских вузов. Входит в топ-5 российских университетов по качеству приема на бюджетные места. Рекордсмен по поступлению олимпиадников в Петербурге. С 2019 года ИТМО самостоятельно присуждает ученые степени кандидата и доктора наук.

СОВРЕМЕННЫЕ МЕТОДЫ И СРЕДСТВА ИССЛЕДОВАНИЙ ТЕПЛОФИЗИЧЕСКИХ СВОЙСТВ ВЕЩЕСТВ

Часть 1

УДК 004.056

ОБОСНОВАНИЕ КРИТЕРИЕВ ОЦЕНКИ РИСКОВ ОРГАНИЗАЦИИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Советова А.С.[1], Сергеева И.Г.[2], Бектибай Б.Ж.[1]
1 – Казахский Национальный Университет имени Аль-Фараби, г. Алматы, Казахстан
2 – Университет ИТМО, Санкт-Петербург, Россия
alua.sovetovaa@mail.ru

Аннотация
В работе рассматривается обоснование критериев оценки рисков организаций в сфере информационной безопасности. Критерий оценки рисков организации в сфере информационной безопасности является важным инструментом для определения и планирования мер по обеспечению безопасности информации. Это позволяет оценить уровень риска, с которым организация сталкивается, и принять соответствующие меры для минимизации рисков. С увеличением количества информации, требующей защиты, растет и угроза ее утечки или кражи. Поэтому, для эффективного управления информационной безопасностью, организации должны осознавать свои риски и проводить их оценку.
Ключевые слова
Информационная безопасность, оценка рисков, риски информационной безопасности.

Перед тем как обосновывать критерий оценки рисков, следует разобраться в понятии самого риска в области информационной безопасности. Риск – это возможность возникновения потерь или негативных последствий, связанных с нарушением конфиденциальности, целостности или доступности информации. Такие последствия могут привести к финансовым потерям, ущербу репутации организации или нарушению законодательства.

Оценка рисков основывается на двух основных компонентах: вероятности возникновения события и величине потерь в случае его осуществления. При этом критерий оценки рисков должен быть объективным, учитывать все возможные угрозы и уязвимости, а также адаптироваться под конкретные условия и потребности организации.

Ниже в таблице указаны проблемные области в сфере информационной безопасности для активов организации.

Таблица

Проблемные области активов организации в сфере информационной безопасности [1]

№	Актив	Виды рисков
1	Аппаратное обеспечение	Потеря электроснабжения из-за временного обесточивания или неисправности оборудования электроснабжения
2		Повреждение компонентов устройства в связи с периодом использования

продолжение таблицы

№	Актив	Виды рисков
3	Программное обеспечение	Ошибка установки приложения из-за неподдерживаемой совместимости пользовательских устройств
4		Отсутствие контроля и надзора за использованием приложений на рабочих устройствах
5	Система	Сбой системы из-за обновления версии приложения/ОС
6		Нарушение работоспособности системы из-за ошибочных действий пользователя при использовании системы
7	Информация	Небрежность пользователя в написании его имени и пароля на физических/цифровых документах, которые попали в широкий доступ
8		Использование утекших паролей

Обоснование критерия оценки рисков организации в сфере информационной безопасности включает следующие аспекты:

1. Первым шагом является идентификация угроз, которые могут повлиять на информационную безопасность организации. Это могут быть внешние атаки, внутренние угрозы, естественные катастрофы и другие факторы, способные нанести вред информационным ресурсам организации.
2. Далее необходимо проанализировать уязвимости системы информационной безопасности организации. Уязвимости могут быть связаны с необходимостью использования устаревшего программного обеспечения, отсутствием политик и процедур, недостаточной квалификацией сотрудников и так далее.
3. При оценке рисков важно учитывать степень возможных последствий, которые могут быть связаны с каждой угрозой. Это могут быть финансовые потери, затруднения в работе, ответственность перед третьими лицами, потеря репутации и другие последствия.
4. Необходимо также учесть вероятность наступления каждого события. Это может быть определено на основе статистических данных, истории инцидентов или экспертных оценок.
5. Критерий оценки рисков должен предоставлять возможность классифицировать риски по их приоритетности и определить необходимые меры по управлению рисками. Например, риски, которые имеют высокую вероятность возникновения и значительные последствия, должны рассматриваться как приоритетные.
6. Наконец, критерий оценки рисков должен быть прозрачным, позволяющим легко интерпретировать результаты оценки и принимать решения по управлению рисками. Он должен быть документирован и доступен для всех заинтересованных сторон.

Чтобы минимизировать информационные риски и повысить уровень информационной безопасности нужны модели для решений проблем. Octave Allegro очень подходит для сертификация управления безопасностью информационных систем для компании, где проводится экспериментальная выяснения того, как активы хранятся, транспортируются и обрабатываются, и как в результате на них влияют угрозы, уязвимости и вмешательство [1, 2].

В предлагаемой модели необходимо выполнить 3 слоя процессов (рисунок), но сначала необходимо идентифицировать все активы в компании [3-6].

Рисунок. Модель поддержки принятия решений в области кибербезопасности

Подводя итог, анализ рисков и оценка соответствия требованиям кибербезопасности могут помочь нам в разработке политик для эффективной и действенной разработки систем безопасности информационных технологий. Обоснование критерия оценки рисков в сфере информационной безопасности является важным шагом для эффективного управления рисками. Это позволяет организации определить наиболее критические угрозы и уязвимости, а также принять меры по управлению ими. Это способствует обеспечению безопасности информации, сохранению репутации организации и минимизации потерь.

Литература

1. Razikin K., Soewito B. Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework, Egyptian Informatics Journal 23. 2022. Pp. 383–404.
2. Tewari A., Comparison between ISO 27005, OCTAVE & NIST SP 800-30, sisainfosec.com, 2020. Comparison between ISO 27005, OCTAVE & NIST SP 800- 30 (accessed Mar. 10, 2021).
3. Fielder A., Panaousis E., Malacaria P., Hankin C., Smeraldi F. Decision support approaches for cyber security investment Decis. Support. Syst., 86. 2016. Pp. 13-23, 10.1016/j.dss.2016.02.012.
4. M'manga A., Faily S., McAlaney J., Williams C., Kadobayashi Y., Miyamoto D. A normative decision-making model for cyber security ICS, 27 (5). 2019. Pp. 636-646.
5. Paul J.A., Zhang M. Decision support model for cybersecurity risk planning: A two-stage stochastic programming framework featuring firms, government, and attacker Eur. J. Oper. Res., 291 (1). 2021. Pp. 349-364, 10.1016/j.ejor.2020.09.013.
6. Achmadi D., Suryanto Y., Ramli K. On developing information security management system (ISMS) Framework for ISO 27001-based Data Center. 2018.