1. American Psychological Association. (2023). Health advisory on social media use in adolescence. https://www.apa.org/topics/social-media-internet/health-advisory-adolescent-social-media-use

2. Ebster, M., Lauerer, M., Nagel, E., & Schmidt, S. (2026). Taming the endless scroll? Short-form videos, digital routines and neurocognitive outcomes in youth: A systematic literature review. European Child & Adolescent Psychiatry, 35, 2727–2743. https://doi.org/10.1007/s00787-026-03083-7

3. Miao, F., & Holmes, W. (2023). Guidance for generative AI in education and research. UNESCO. https://unesdoc.unesco.org/

4. Naik, V. S., Mathias, E. G., Krishnan, P., & Jagannath, V. (2025). Impact of social media on cognitive development of children and young adults: A systematic review. BMC Pediatrics, 25, 826. https://doi.org/10.1186/s12887-025-06041-5

5. Ophir, E., Nass, C., & Wagner, A. D. (2009). Cognitive control in media multitaskers. Proceedings of the National Academy of Sciences, 106(37), 15583–15587. https://doi.org/10.1073/pnas.0903620106

6. Sweller, J. (1988). Cognitive load during problem solving: Effects on learning. Cognitive Science, 12(2), 257–285. https://doi.org/10.1207/s15516709cog1202_4

УПРАВЛЕНИЕ КИБЕРРИСКАМИ ОРГАНИЗАЦИЙ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ: ИННОВАЦИОННАЯ МОДЕЛЬ ОЦЕНКИ УГРОЗ И ОБЕСПЕЧЕНИЯ УСТОЙЧИВОГО РАЗВИТИЯ

Ахматова Нигора Нурулло кизи
Независимый исследователь, Ташкент, Республика Узбекистан
E-mail: nigoraa479@gmail.com

Аннотация. В статье рассматриваются проблемы обеспечения информационной безопасности организаций в условиях цифровой трансформации и их влияние на устойчивость организационной деятельности. Расширение применения информационных систем, облачных технологий, сетевой инфраструктуры и цифровых сервисов сопровождается увеличением количества потенциальных киберугроз и уязвимостей. Цель исследования заключается в разработке риск-ориентированной модели оценки киберугроз, позволяющей определять приоритетность угроз с учетом вероятности их реализации, потенциального ущерба и критичности информационных активов. Методологическую основу составляют сравнительный анализ международных стандартов ISO/IEC 27001, ISO/IEC 27005 и рекомендаций NIST Cybersecurity Framework 2.0, методы системного анализа, классификации угроз и количественной оценки рисков. Предложена многоуровневая модель, включающая идентификацию информационных активов, классификацию угроз, расчет интегрального показателя риска и выбор приоритетных мер защиты. Практическая значимость модели состоит в возможности ее применения для повышения устойчивости цифровой инфраструктуры и рационального распределения ресурсов организации.

Ключевые слова: информационная безопасность, киберугрозы,

киберриски, цифровая трансформация, информационные системы, оценка рисков, устойчивое развитие, ISO/IEC 27001, NIST CSF 2.0.

1. Введение

Современный этап социально-экономического развития характеризуется активным внедрением цифровых технологий в деятельность государственных учреждений, промышленных предприятий, финансовых организаций и коммерческих структур. Информационные системы становятся важнейшим инструментом управления производственными процессами, обработки данных, организации коммуникаций и принятия управленческих решений.

Вместе с тем цифровая трансформация приводит к усложнению информационной инфраструктуры организаций. Использование облачных платформ, распределенных информационных систем, удаленного доступа и интегрированных цифровых сервисов расширяет потенциальную поверхность кибератак.

К числу наиболее значимых угроз относятся вредоносное программное обеспечение, фишинговые атаки, несанкционированный доступ, утечки конфиденциальной информации, атаки типа «отказ в обслуживании» (DDoS), а также эксплуатация уязвимостей программного и аппаратного обеспечения.

Особую опасность представляют комплексные инциденты информационной безопасности, способные одновременно нарушить доступность информационных ресурсов, целостность данных и конфиденциальность информации.

В этих условиях традиционный подход, основанный преимущественно на установке отдельных технических средств защиты, не всегда обеспечивает необходимый уровень безопасности. Возникает необходимость перехода к риск-ориентированному управлению, при котором защитные мероприятия определяются на основании систематической оценки угроз и потенциального ущерба.

Таким образом, разработка модели количественной оценки киберугроз является актуальной научно-практической задачей.

2. Анализ существующих подходов к управлению информационной безопасностью

В международной практике сформировалось несколько основных подходов к обеспечению информационной безопасности.

Стандарт ISO/IEC 27001:2022 определяет требования к созданию, внедрению, поддержанию и постоянному совершенствованию системы менеджмента информационной безопасности (СМИБ).

ISO/IEC 27005:2022 ориентирован на управление рисками информационной безопасности и предусматривает процессы идентификации, анализа, оценки и обработки рисков.

NIST Cybersecurity Framework 2.0, опубликованный в 2024 году, предлагает системный подход к управлению кибербезопасностью на основе шести основных функций: Govern (управление), Identify (идентификация), Protect (защита), Detect (обнаружение), Respond (реагирование) и Recover

(восстановление).

Несмотря на различия в методологических подходах, перечисленные документы объединяет принцип системного и непрерывного управления информационной безопасностью.

Вместе с тем для практического применения необходима модель, позволяющая не только выявлять потенциальные угрозы, но и количественно определять их приоритетность с учетом особенностей конкретной организации.

Для решения данной задачи предлагается использовать интегрированную модель, объединяющую классификацию информационных активов, анализ угроз, оценку уязвимостей и расчет уровня риска.

3. Разработка риск-ориентированной модели оценки киберугроз

Предлагаемая модель основана на последовательном выполнении пяти взаимосвязанных этапов.

Первый этап — идентификация информационных активов.

– серверное оборудование и сетевые устройства;
– базы данных и электронные документы;
– корпоративные информационные системы;
– программное обеспечение;
– учетные записи пользователей;
– каналы передачи информации.

Для каждого актива определяется его критичность с учетом влияния возможного нарушения конфиденциальности, целостности и доступности информации.

Второй этап — идентификация и классификация киберугроз.

1. Технические угрозы — уязвимости программного обеспечения, отказы оборудования, сетевые атаки.
2. Программные угрозы — вредоносное ПО, программы-вымогатели, эксплуатация ошибок программного кода.
3. Сетевые угрозы — перехват трафика, несанкционированное подключение, DDoS-атаки.
4. Пользовательские угрозы — фишинг, компрометация учетных записей, ошибки персонала.
5. Организационные угрозы — недостатки политики безопасности, отсутствие контроля доступа и несвоевременное обновление систем.

Третий этап — количественная оценка риска.

$$\mathbf{R_i = P_i \times I_i}$$

где R_i — уровень риска для i-й угрозы; P_i — вероятность реализации угрозы; I_i — потенциальное воздействие (ущерб) при реализации угрозы.

Для практической оценки предлагается использовать пятибалльную шкалу: вероятность реализации угрозы — от 1 до 5; степень потенциального ущерба — от 1 до 5. В результате максимальное значение риска составляет 25 баллов.

Для дополнительного учета критичности информационного актива предлагается расширенная модель:

$$R_i = P_i \times I_i \times K_i$$

где K_i — коэффициент критичности информационного актива в диапазоне от 0,2 до 1,0. Чем выше значение коэффициента, тем более значимым является актив для функционирования организации.

Четвертый этап — определение приоритетности рисков.

Значение риска	Уровень	Рекомендуемое действие
1–5	Низкий	Мониторинг
6–10	Умеренный	Плановые меры защиты
11–15	Высокий	Приоритетное снижение риска
16–25	Критический	Незамедлительное реагирование

Указанные пороговые значения представляют собой предлагаемую рабочую классификацию и должны уточняться с учетом отрасли и политики управления рисками организации.

Пятый этап — выбор и реализация защитных мероприятий.

– многофакторная аутентификация;
– разграничение прав доступа;
– сегментация корпоративной сети;
– регулярное обновление программного обеспечения;
– резервное копирование данных;
– применение средств обнаружения и предотвращения вторжений;
– мониторинг событий информационной безопасности;
– обучение сотрудников методам противодействия фишинговым атакам.

После внедрения защитных мероприятий проводится повторная оценка рисков.

4. Математическая интерпретация предлагаемой модели

Рассмотрим условный пример оценки трех потенциальных угроз для информационной инфраструктуры организации.

№	Киберугроза	тность P	Ущерб I	Критичность K
1	Фишинговая атака	4	4	0,8
2	DDoS-атака	3	5	0,9
3	Утечка учетных данных	4	5	1,0

Расчет осуществляется по формуле $R_i = P_i \times I_i \times K_i$. Получаем:

– Фишинговая атака: $4 \times 4 \times 0{,}8 = 12{,}8$.
– DDoS-атака: $3 \times 5 \times 0{,}9 = 13{,}5$.
– Утечка учетных данных: $4 \times 5 \times 1{,}0 = 20$.

Таким образом, наибольшее значение риска в рассматриваемом условном примере соответствует угрозе утечки учетных данных.

Это означает, что организация должна в первую очередь рассмотреть внедрение дополнительных механизмов аутентификации, контроля доступа,

мониторинга пользовательской активности и защиты учетных записей.

Следует отметить, что приведенные значения являются иллюстративными и не представляют результаты обследования реального предприятия.

5. Практическая значимость и возможности применения модели

Предлагаемая модель может применяться в организациях различных отраслей экономики, включая промышленность, образование, банковский сектор, телекоммуникации и государственное управление.

Ее практическое использование позволяет:

– систематизировать информацию об информационных активах;
– выявлять наиболее опасные киберугрозы;
– определять приоритетные направления технической защиты;
– рационально распределять ресурсы на обеспечение кибербезопасности;
– оценивать изменение уровня рисков после реализации защитных мероприятий.

Дополнительным направлением развития модели является ее интеграция с автоматизированными системами мониторинга информационной безопасности (SIEM), системами управления уязвимостями и средствами анализа сетевого трафика.

В перспективе применение методов машинного обучения позволит учитывать динамику киберугроз, выявлять аномальное поведение пользователей и повышать точность оценки вероятности реализации атак.

При этом автоматизированная оценка должна дополнять, а не полностью заменять экспертный анализ и систематическое управление информационными рисками.

6. Заключение

В результате проведенного исследования рассмотрены основные проблемы обеспечения информационной безопасности организаций в условиях цифровой трансформации.

Проанализированы международные подходы к управлению информационной безопасностью, представленные стандартами ISO/IEC 27001:2022, ISO/IEC 27005:2022 и NIST Cybersecurity Framework 2.0.

Предложена риск-ориентированная модель оценки киберугроз, основанная на идентификации информационных активов, классификации угроз, количественной оценке вероятности их реализации и потенциального ущерба.

Основным элементом модели является математическая зависимость, учитывающая вероятность угрозы, величину возможного ущерба и критичность защищаемого информационного актива.

Научная новизна предлагаемого подхода состоит в объединении оценки вероятности реализации угрозы, потенциального ущерба и коэффициента критичности информационного актива в едином расчетном показателе для ранжирования киберрисков. Практическая значимость заключается в возможности использовать эту модель как основу для определения

приоритетных мер защиты и более обоснованного распределения ресурсов организации.

Дальнейшие исследования целесообразно направить на экспериментальную проверку модели в реальной информационной инфраструктуре, разработку алгоритмов автоматизированного расчета рисков и оценку эффективности предлагаемых защитных мероприятий.

Таким образом, риск-ориентированная модель может стать методологической основой для совершенствования систем информационной безопасности организаций и повышения устойчивости их цифровой инфраструктуры.

Список использованной литературы

1. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva: International Organization for Standardization, 2022.
2. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks. Geneva: International Organization for Standardization, 2022.
3. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Gaithersburg, MD, 2024. DOI: 10.6028/NIST.CSWP.29.
4. NIST Special Publication 800-30 Revision 1. Guide for Conducting Risk Assessments. National Institute of Standards and Technology, 2012. DOI: 10.6028/NIST.SP.800-30r1.
5. NIST Special Publication 800-61 Revision 2. Computer Security Incident Handling Guide. National Institute of Standards and Technology, 2012. DOI: 10.6028/NIST.SP.800-61r2.
6. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls. Geneva: International Organization for Standardization, 2022.

CHO‘L HUDUDLARIDAGI DORIVOR O‘SIMLIKLARDAN OQILONA FOYDALANISH VA ULARNI MUHOFAZA QILISHNING YASHIL IQTISODIYOTDAGI AHAMIYATI

Pardayeva E’zoza Olim qizi, O‘ralov Abdumanon Iskandarovich., Nematova Maloxat Abdurasulovna
Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy Universiteti Jizzax filiali
E-mail: pardayeva.ezoza@nuu.uz

Annotatsiya: Ushbu maqolada cho‘l hududlarida tarqalgan dorivor o‘simliklarning ekologik, iqtisodiy va biologik ahamiyati, ulardan oqilona foydalanish hamda tabiiy resurslarni muhofaza qilish masalalari yoritilgan. Shuningdek, yashil iqtisodiyot tamoyillari asosida dorivor o‘simliklarni yetishtirish, qayta ishlash, biologik xilma-xillikni saqlash va ekologik barqarorlikni ta’minlash imkoniyatlari tahlil qilingan. O‘zbekistonning qurg‘oqchil hududlarida uchraydigan