РИСКИ КИБЕРБЕЗОПАСНОСТИ И МЕХАНИЗМЫ УПРАВЛЕНИЯ

Научный руководитель: Ишманова Динара, DSc,

Ректор Университета Миллат Умиди,

Студент 4 курса Университета Миллат Умиди,

Шохжахон Усманбеков Даниёрович

Аннотация статьи: В данной статье анализируются риски кибербезопасности и механизмы управления ими как актуальная проблема современного информационного общества. В исследовании рассматриваются основные киберугрозы, возникающие с развитием цифровых технологий, – кража данных, вредоносное ПО, фишинговые атаки, распределенный отказ в обслуживании (DDoS) и внутренние угрозы. Также освещается роль международного опыта, национального законодательства, политики информационной безопасности, повышения цифровой грамотности сотрудников и использования современных технических средств в обеспечении кибербезопасности. В статье на основе анализа научных трудов зарубежных и узбекских ученых, опубликованных в 2021–2025 годах, разрабатываются эффективные подходы и практические механизмы управления кибербезопасностью. Результаты исследования служат для разработки рекомендаций по формированию культуры информационной безопасности в организациях и снижению рисков.

Ключевые слова: Кибербезопасность, анализ угроз, управление рисками, защита информационных систем, киберзащита от «ИИ».

Maqola annotatsiyasi: Ushbu maqolada kiberxavfsizlik risklari va ularni boshqarish mexanizmlari zamonaviy axborot jamiyatida dolzarb masala sifatida tahlil qilinadi. Tadqiqotda raqamli texnologiyalar rivoji bilan yuzaga kelayotgan asosiy kiberxavflar — ma’lumotlar o‘g‘irlanishi, zararli dasturlar, fishing hujumlari, tarmoqlarni ishdan chiqarish (DDoS) va ichki tahdidlar kabi xavf turlari ko‘rib chiqilgan. Shuningdek, kiberxavfsizlikni ta’minlashda xalqaro tajriba, milliy qonunchilik, axborot xavfsizligi siyosati, xodimlarning raqamli savodxonligini oshirish hamda zamonaviy texnik vositalardan foydalanishning o‘rni yoritilgan. Maqolada 2021–2025-yillarda chop etilgan xorijiy va o‘zbek olimlarining ilmiy ishlari tahlili asosida kiberxavfsizlikni boshqarishning samarali yondashuvlari va

amaliy mexanizmlari ishlab chiqilgan. Tadqiqot natijalari tashkilotlarda axborot xavfsizligi madaniyatini shakllantirish va risklarni kamaytirish bo‘yicha tavsiyalar ishlab chiqishga xizmat qiladi.

Kalit so‘zlar: Kiberxavfsizlik, xavf tahlili, risklarni boshqarish, axborot tizimlari himoyasi, “AI”dan kiberhimoya.

CYBERSECURITY RISKS AND MANAGEMENT MECHANISMS

Supervisor: Dinara Ishmanova, DSc,

Rector of Millat Umidi University,

Fourth-year student at Millat Umidi University,

Shohjahon Usmanbekov Danijorovich

Annotation: This article analyzes cybersecurity risks and their management mechanisms as a pressing issue in the modern information society. The study examines the main cyberthreats arising with the development of digital technologies, including data theft, malware, phishing attacks, distributed denial of service (DDoS), and insider threats. It also highlights the role of international experience, national legislation, information security policies, improving employee digital literacy, and the use of modern technical tools in ensuring cybersecurity. Based on an analysis of scientific papers by international and Uzbek scholars published between 2021 and 2025, the article develops effective approaches and practical mechanisms for cybersecurity management. The results of the study serve to develop recommendations for developing an information security culture in organizations and mitigating risks.

Key words: Cybersecurity, threat analysis, risk management, information systems protection, cyber defense against AI.

Введение: В современную эпоху глобализации и цифровых технологий информационные системы глубоко проникают во все сферы деятельности человека. При этом вопросы безопасности в цифровой среде, в частности риски кибербезопасности, становятся актуальной проблемой. Кибербезопасность – это сложная система мер, направленных на защиту информационных ресурсов от несанкционированного доступа, повреждения, кражи или потери. Рост числа и сложности кибератак в последние годы представляет большую угрозу для государственных органов, субъектов

предпринимательства и рядовых пользователей. В Республике Узбекистан в рамках стратегии «Цифровой Узбекистан – 2030» проводится системная работа по укреплению информационной безопасности, развитию национальной инфраструктуры компьютерную безопасность и внедрению механизмов управления, соответствующих международным стандартам. В этой связи выявление, оценка и разработка эффективных механизмов управления рисками информационная безопасность становятся неотъемлемой частью современной управленческой практики. Данная статья посвящена данному вопросу – теоретическим и практическим аспектам снижения рисков компьютерную безопасность и управления ими.

Обзор литературы: Зарубежный учёный Дж. Уильямс (2022) в своём исследовании проанализировал уязвимости цифровых инфраструктур и подчеркнул необходимость использования технологий искусственного интеллекта для их выявления. Также **Р. Чен и Л. Парк (2023)** научно обосновали эффективность проактивной модели управления рисками при разработке стратегий безопасность информационных технологий. По их мнению, раннее выявление источников киберрисков и мониторинг рисков в режиме реального времени существенно повышают безопасность организации.

Узбекский учёный А. Холматов (2022) отметил важность гармонизации национальных стандартов и международных требований при формировании системы информационная безопасность. По его словам, сотрудничество государства и частного сектора является одним из основных факторов предотвращения кибератак. **Д. Джоураев (2023)** также подчеркнул необходимость повышения кадрового потенциала, развития культуры информационной безопасности и обновления технической инфраструктуры в обеспечении информационная безопасность в нашей стране.

На **международном уровне Э. Браун (2024)** рассматривает кибербезопасность как неотъемлемую часть экономической безопасности в контексте цифровой экономики. Он анализирует непосредственное влияние факторов киберриска на экономическую стабильность и обосновывает необходимость комплексного подхода к управлению ими.

Методология исследования: В качестве методических методов исследования были использованы аналитический подход, статистический

анализ данных, графический анализ, сравнение с передовым зарубежным опытом и научное обобщение.

Анализ и результаты: Риски кибербезопасности и преимущества управления: Внедрение механизмов управления рисками кибербезопасности дает организациям, государственным органам и обществу ряд важных преимуществ. Прежде всего, эти системы позволяют надежно защищать информационные ресурсы и предотвращать кибератаки. **Обеспечивается безопасность данных,** что предотвращает утечку или порчу конфиденциальной информации. Гарантируется непрерывность бизнес-процессов. **Механизмы безопасность информационных технологий сокращают время простоя систем,** что обеспечивает стабильную работу бизнес-процессов. Они служат повышению доверия клиентов и партнеров. Высокий уровень информационной безопасности организации повышает ее конкурентоспособность. Система управления кибербезопасностью снижает финансовые потери. Существенно сокращаются ущерб, штрафы или репутационный ущерб, наносимый кибератаками. Повышение цифровой грамотности сотрудников формирует в организации культуру безопасности.

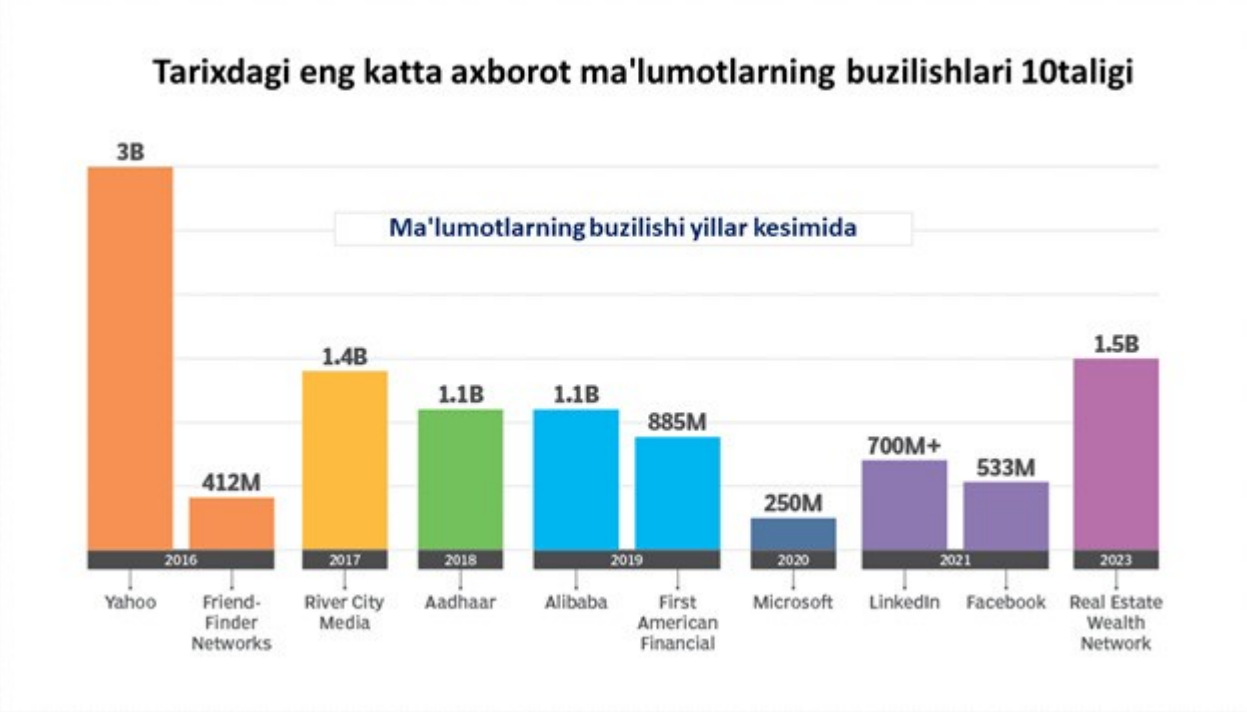

Диаграмма 1. Крупнейшие утечки данных в истории

Источник: https://infocom.uz/articles/cybersecurity-statistics

Графический анализ: Количество атак вредоносных программ увеличилось на 71% в период с 2016 по 2021 год. Число жертв атак программ-вымогателей увеличилось на 128,17% в период с 2022 по 2023 год. 4,1 миллиона сайтов были навсегда заражены вредоносным ПО.

Риски кибербезопасности и слабые стороны механизмов управления: Высокие затраты - внедрение современных систем защиты, программного и аппаратного обеспечения требует значительных финансовых ресурсов, что создает трудности для малых и средних предприятий. **Нехватка специалистов** - в результате нехватки квалифицированных кадров в области компьютерную безопасность могут возникать ошибки в процессах анализа и управления рисками. **Сложность адаптации к быстро меняющейся среде угроз** - киберпреступники постоянно используют новые методы, что приводит к устареванию существующих систем защиты в короткие сроки. Из-за низкой культуры информационной безопасности в некоторых организациях халатность или некорректные действия сотрудников создают внутренние источники риска. **Недостаточно развитая нормативно-правовая база также снижает эффективность управления кибербезопасностью,** поскольку в ряде случаев механизмы ответственности за киберпреступления четко не определены. Проблемы интеграции между различными системами и трудности в согласовании политик безопасности также являются существенными недостатками.

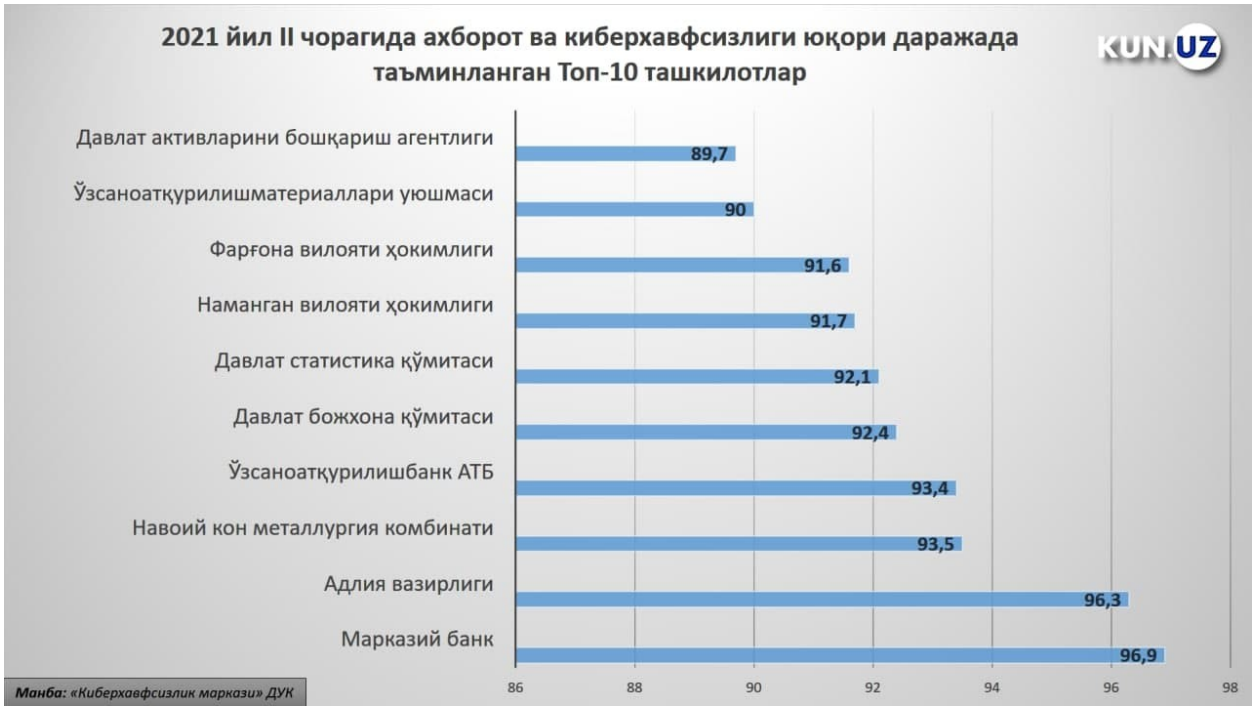

Диаграмма 2. Организации с высоким уровнем информационной и кибербезопасности в 2021 году

Источник: https://kun.uz/45263052?q=%2F45263052#!

Графический анализ: Центральный банк занял первое место в рейтинге центра, набрав 96,9 балла. Министерство юстиции заняло следующее место.

Навоийский горно-металлургический комбинат, производящий золото — основной экспортный товар Узбекистана, замкнул тройку лидеров по уровню информационной и кибербезопасности.

В первую десятку также вошли таможенный и статистический комитеты, хокимияты Наманганской и Ферганской областей.

Предложения: Улучшение национальной стратегии кибербезопасности - Необходимо сформировать единую государственную политику в области компьютерную безопасность, внедрить единые стандарты и протоколы для всех отраслей. **Развивать систему подготовки кадров** – необходимо расширить направления информационной безопасности в высших учебных заведениях, создать практико-ориентированные учебные программы и организовать курсы повышения квалификации специалистов. **Внедрять искусственный интеллект и автоматизированные системы мониторинга** – важно широко использовать современные технологии для раннего обнаружения, анализа и оперативного реагирования на киберугрозы. **Укреплять сотрудничество между частным сектором и государством** – рекомендуется обеспечить системный подход путем создания единой платформы для обмена информацией, мониторинга и предотвращения угроз. **Формировать культуру информационной безопасности у сотрудников** – количество ошибок, вызванных человеческим фактором, можно снизить путем регулярного проведения тренингов, семинаров и симуляционных учений по киберугрозам. **Совершенствование нормативно-правовой базы** – необходимо актуализировать механизмы борьбы с киберпреступностью и наказания в соответствии с международными стандартами, а также обеспечить правовое сопровождение деятельности организаций, осуществляющих кибербезопасность. Реализация данных предложений позволит обеспечить системный подход к кибербезопасности и повысить устойчивость информационной безопасности на национальном и корпоративном уровнях.

Заключение: В заключение следует отметить, что управление рисками компьютерную безопасность является одним из важнейших стратегических направлений в современном цифровом обществе. В условиях роста кибератак, стремительного развития технологий и расширения информационных потоков потребность организаций в совершенствовании своих систем безопасности возрастает с каждым днем. Эффективные механизмы управления кибербезопасностью важны не только для защиты данных, но и для обеспечения экономической стабильности, повышения доверия клиентов и создания среды цифрового доверия. Анализ показывает, что для достижения успеха в области компьютерную безопасность необходимо комплексное применение технических, организационных и правовых мер. Основными факторами являются использование искусственного интеллекта и автоматизированных систем, повышение кадрового потенциала и формирование культуры информационной безопасности.

Список использованной литературы:

1. Уильямс, Дж. (2022). Оценка рисков кибербезопасности и обнаружение угроз с помощью ИИ. Журнал исследований информационной безопасности, т. 15(2), стр. 45–59.
2. Чен, Р. и Парк, Л. (2023). Структура проактивного управления киберрисками для цифровых предприятий. Международный журнал кибербезопасности и цифрового доверия, том 9(1), стр. 112–128.
3. Браун, Э. (2024). Кибербезопасность как компонент экономической стабильности в цифровую эпоху. Global Technology Review, т. 12(3), стр. 75–90.
4. Холматов, А. (2022). Организационно-правовые основы совершенствования системы кибербезопасности в условиях Узбекистана. Журнал информационных технологий, № 4, с. 23–31.
5. Джораев, Д. (2023). «Роль человеческих ресурсов и цифровой культуры в обеспечении кибербезопасности». Инновационное развитие и информационная безопасность, № 2, стр. 17–25.
6. Указ Президента Республики Узбекистан от 5 октября 2020 года № УФ-6079 «Об утверждении стратегии «Цифровой Узбекистан – 2030».

7. Международный союз электросвязи (МСЭ). (2023). Глобальный индекс кибербезопасности 2023. Женева: Издательство МСЭ.
8. Национальный институт стандартов и технологий (NIST). (2022). Основы повышения кибербезопасности критически важной инфраструктуры (версия 2.0). Министерство торговли США.
9. Рахмонов, Б. (2024). «Роль технологий искусственного интеллекта в управлении политикой информационной безопасности». Журнал информационных систем Узбекистана, № 1, стр. 42–50.
10. Агентство Европейского союза по кибербезопасности (ENISA). (2023). Отчёт о ландшафте угроз кибербезопасности. Брюссель: ENISA.
11. https://infocom.uz/articles/cybersecurity-statistics
12. https://kun.uz/45263052?q=%2F45263052#!