SCIENTIFIC CONFERENCE OPEN PROCEEDINGS
Global Academic Knowledge Repository

АКТУАЛЬНЫЕ ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В РЕСПУБЛИКЕ УЗБЕКИСТАН

Курбонова Фируза Зариповна

Доктор философии по техническим наукам, доцент, Академия Министерства внутренних дел Республики Узбекистан, Ташкент, Узбекистан

https://doi.org/10.5281/zenodo.20955567

Annotatsiya. Mazkur maqolada O‘zbekiston Respublikasida kiberxavfsizlikni ta’minlashning dolzarb muammolari, mavjud tahdidlar va ularni bartaraf etishning zamonaviy yondashuvlari tahlil qilinadi. Davlat axborot tizimlari va muhim axborot infratuzilmalari xavfsizligini ta’minlash, kiberjinoyatchilikka qarshi kurashish, milliy kiberxavfsizlik tizimini rivojlantirish hamda xalqaro tajribalarni joriy etish masalalari yoritilgan. Shuningdek, mamlakatda kiberxavfsizlik sohasini rivojlantirish istiqbollari va ushbu yo‘nalishda amalga oshirilishi zarur bo‘lgan chora-tadbirlar ilmiy jihatdan asoslab berilgan.

Kalit so‘zlar: kiberxavfsizlik, axborot xavfsizligi, kiberjinoyatchilik, raqamli transformatsiya, muhim axborot infratuzilmasi, davlat axborot tizimlari, kibertahdid.

Аннотация. В данной статье рассматриваются актуальные проблемы обеспечения кибербезопасности в Республике Узбекистан, существующие киберугрозы и современные подходы к их предотвращению. Проанализированы вопросы защиты государственных информационных систем и объектов критической информационной инфраструктуры, противодействия киберпреступности, развития национальной системы кибербезопасности и внедрения международного опыта. Кроме того, определены перспективные направления развития сферы кибербезопасности в

условиях цифровой трансформации, а также научно обоснованы меры по повышению уровня защищённости информационных ресурсов государства.

Ключевые слова: кибербезопасность, информационная безопасность, киберпреступность, цифровая трансформация, критическая информационная инфраструктура, государственные информационные системы, киберугрозы.

Abstract. This article examines the current challenges and future prospects of ensuring cybersecurity in the Republic of Uzbekistan. It analyzes cyber threats, the protection of government information systems and critical information infrastructure, and measures to combat cybercrime. The paper also discusses the development of the national cybersecurity system, the implementation of international best practices, and the key priorities for strengthening cybersecurity in the context of digital transformation.

Keywords: cybersecurity, information security, cybercrime, digital transformation, critical information infrastructure, cyber threats.

Введение

В результате развития цифровой экономики и систем электронного государственного управления информационно-коммуникационные технологии активно внедряются во все сферы деятельности страны. Перевод государственных услуг в электронный формат, цифровизация банковской системы, широкое внедрение электронной коммерции и облачных технологий приводят к значительному увеличению объёма информационных ресурсов [3].

Наряду с этими процессами также растут такие угрозы, как киберпреступность, несанкционированный доступ, вредоносные программы, фишинговые атаки, DDoS-атаки и утечки данных. В связи с этим обеспечение национальной кибербезопасности является одним из приоритетных направлений государственной политики.

Современное состояние кибербезопасности в Узбекистане

В последние годы в стране реализуются важные реформы по обеспечению информационной безопасности. Совершенствуются нормативно-правовые основы в области защиты информационных систем государственных органов, развития инфраструктуры электронного правительства, обеспечения безопасности государственных информационных ресурсов и противодействия киберпреступности [7].

Однако с увеличением количества информационных систем также возрастает число потенциальных уязвимостей. В особенности государственные информационные системы, подключённые к сети Интернет, банковские сервисы, мобильные приложения и корпоративные сети постоянно остаются объектами внимания киберпреступников [8].

Существующие проблемы кибербезопасности

Человеческий фактор - Большая часть киберинцидентов связана с недостаточным уровнем знаний и навыков пользователей. Использование слабых паролей, переход по фишинговым ссылкам, загрузка вредоносных файлов и другие неосторожные действия могут привести к нарушению безопасности информационных систем.

Технические уязвимости

Во многих организациях встречаются следующие проблемы:

- использование устаревшего программного обеспечения;
- применение нелицензионных программ;
- несвоевременная установка обновлений безопасности;
- неправильная настройка сетевой инфраструктуры.

Наличие таких недостатков повышает вероятность успешного проведения кибератак и может привести к утечке конфиденциальной информации.

Недостаток квалифицированных специалистов

Потребность в высококвалифицированных специалистах в области кибербезопасности постоянно возрастает. Для противодействия современным киберугрозам необходимы специалисты, обладающие не только техническими знаниями, но и правовыми, аналитическими навыками. Подготовка профессиональных кадров является одним из ключевых факторов обеспечения эффективной защиты информационных систем [1], [2].

Правовые проблемы

Трансграничный характер киберпреступлений значительно усложняет процесс их выявления, расследования и привлечения виновных лиц к ответственности. В связи с этим важное значение имеет развитие международного сотрудничества, обмен опытом и совершенствование механизмов взаимодействия между государствами в сфере противодействия киберугрозам [3].

Современные киберугрозы

В настоящее время наиболее актуальными угрозами в сфере кибербезопасности являются:

- атаки с использованием программ-вымогателей (**ransomware**);
- фишинговые и целевые фишинговые атаки (**phishing и spear phishing**);
- DDoS-атаки [2];
- внутренние угрозы (**Insider Threat**) [4];
- атаки, осуществляемые с использованием технологий искусственного интеллекта;
- угрозы, направленные на устройства Интернета вещей (**IoT**);
- атаки на облачную инфраструктуру.

Данные угрозы требуют постоянного совершенствования методов защиты, внедрения современных технологий мониторинга и повышения уровня информационной грамотности пользователей [3].

Современные подходы к обеспечению кибербезопасности

Для развития национальной системы кибербезопасности важное значение имеют следующие направления:

- внедрение архитектуры **Zero Trust**;
- использование систем мониторинга на основе технологий искусственного интеллекта;
- развитие центров управления событиями информационной безопасности (**SOC — Security Operations Center**);
- регулярное проведение аудита безопасности и тестирования на проникновение (**Pentest**);
- совершенствование средств криптографической защиты информации;
- повышение уровня кибергигиены и квалификации сотрудников.

Перспективные направления для Узбекистана

В дальнейшем целесообразно реализовать следующие задачи:

- дальнейшее совершенствование национальной стратегии кибербезопасности [1];
- разработка отечественного программного обеспечения и средств защиты информации [2];
- внедрение систем обнаружения киберугроз на основе искусственного интеллекта;
- расширение научных исследований в области кибербезопасности в высших образовательных учреждениях [5];
- широкое внедрение международных стандартов (**ISO/IEC 27001, NIST Cybersecurity Framework**) в практическую деятельность [7];

- усиление обмена информацией между государственным и частным секторами.

Заключение

В условиях цифровой трансформации обеспечение кибербезопасности в Республике Узбекистан становится неотъемлемой частью национальной безопасности. Надёжная защита информационных систем и объектов критической инфраструктуры является важным условием устойчивого развития государственного управления, экономики и общества в целом.

Результаты исследования показывают, что укрепление кибербезопасности не ограничивается только внедрением современных технических средств защиты. Данный процесс также требует совершенствования нормативно-правовой базы, развития международного сотрудничества, подготовки квалифицированных специалистов, поддержки научных исследований и повышения уровня культуры кибергигиены среди пользователей.

В перспективе эффективное использование технологий искусственного интеллекта, больших данных (**Big Data**), облачных технологий и автоматизированных систем мониторинга позволит значительно повысить уровень киберустойчивости страны. Вместе с тем развитие национальной инфраструктуры кибербезопасности на основе международных стандартов, а также укрепление взаимодействия между государственными органами, научными учреждениями и частным сектором будут способствовать безопасному и стабильному развитию Республики Узбекистан в цифровом пространстве.

REFERENCES

1. Закон Республики Узбекистан «О кибербезопасности». Закон Республики Узбекистан от 15 апреля 2022 года № ЗРУ-764. URL: https://lex.uz/docs/5960604
2. Указ Президента Республики Узбекистан «О стратегии “Цифровой Узбекистан – 2030”». URL: https://lex.uz/docs/5030957
3. NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology. URL: https://www.nist.gov/cyberframework (NIST)
4. ISO/IEC 27001:2022. Information Security Management Systems — Requirements. International Organization for Standardization. URL: https://www.iso.org/standard/27001.html
5. ENISA Threat Landscape Report. European Union Agency for Cybersecurity. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape
6. Stallings W. Cryptography and Network Security: Principles and Practice. — 8th Edition. Pearson Education, 2023.
7. Goodfellow I., Bengio Y., Courville A. Deep Learning. — MIT Press, 2016. URL: https://www.deeplearningbook.org/
8. Sarker I.H. Machine Learning: Algorithms, Real-World Applications and Research Directions. — SN Computer Science, 2021.
9. Cisco Cybersecurity Report. Global Cybersecurity Trends and Threats. URL: https://www.cisco.com/c/en/us/products/security/
10. IBM Security X-Force Threat Intelligence Index. URL: https://www.ibm.com/reports/threat-intelligence

11. Kaspersky. Отчёты по киберугрозам и исследованиям информационной безопасности.
URL: https://www.kaspersky.com/resource-center/threats
12. Cybersecurity Ventures. Cybercrime Reports and Research.
URL: https://cybersecurityventures.com/
13. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. — 3rd Edition. Wiley, 2020.
14. Mishra A., Sharma S. Artificial Intelligence Applications in Cybersecurity: A Review. — International Journal of Computer Applications, 2022.
15. Whitman M., Mattord H. Principles of Information Security. — Cengage Learning, 2021.