ACUMEN: INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH
ISSN: 3060-4745 IF(Impact Factor)10.71 / 2025 Volume 3, Issue 4

ЦИФРОВАЯ БЕЗОПАСНОСТЬ: УГРОЗЫ И КАК С НИМИ БОРОТЬСЯ

Ибрагимов Зойиржон Зиятович
Старший преподаватель кафедры «К и ПИ» Джизакского политехнического института. zoyirjon.ibragimov@gmail.com
Ибрагимова Наргиза Аноровна
Старший преподаватель филиала Казанского федерального университета (Приволжский регион) в г. Джизаке. anorovna1791@mail.com

Аннотация: В эпоху цифровизации кибербезопасность становится одной из ключевых проблем современного общества. Быстрое развитие технологий, распространение облачных сервисов, искусственного интеллекта и интернета вещей (IoT) создают новые вызовы для защиты информации. Основными угрозами являются кибератаки, вредоносное ПО, фишинг, утечки данных и взломы систем. В данной работе рассматриваются актуальные угрозы кибербезопасности, методы защиты данных, включая использование криптографии, двухфакторной аутентификации, антивирусного программного обеспечения и принципов безопасного поведения в сети. Особое внимание уделяется роли государственных и корпоративных стратегий в обеспечении цифровой безопасности [1].

Ключевые слова: кибербезопасность, цифровизация, угрозы, защита данных, кибератаки, информационная безопасность.

Введение: Современный мир все больше зависит от цифровых технологий, что приводит к росту угроз в области кибербезопасности. Расширение цифровой трансформации, облачных сервисов, искусственного интеллекта и интернета вещей (IoT) создает новые вызовы для защиты данных. В данной статье рассматриваются основные киберугрозы и эффективные способы защиты информации в условиях цифровизации.

Основные угрозы кибербезопасности: Угрозы кибербезопасности – это потенциальные или реальные действия злоумышленников, которые могут привести к утечке, потере, повреждению или краже данных, а также нарушению работы цифровых систем [4,5]. Эти угрозы могут быть направлены как на отдельных пользователей, так и на компании, организации или даже государственные структуры.

ISSN: 3060-4745 IF(Impact Factor)10.71 / 2025 Volume 3, Issue 4

Киберугрозы могут проявляться в различных формах, включая вредоносное программное обеспечение, фишинг, взлом систем, атаки на сети и утечки конфиденциальной информации. Основная цель таких атак – получить несанкционированный доступ к данным, нанести финансовый ущерб, нарушить работу организаций или подорвать доверие к цифровым технологиям.

Чтобы эффективно противостоять этим угрозам, необходимо применять современные методы защиты, такие как шифрование данных, двухфакторная аутентификация, антивирусное ПО и регулярное обновление систем безопасности.

С развитием технологий появляются новые виды атак, представляющие серьезную опасность для пользователей и организаций. Рассмотрим основные из них:

Кибератаки – направленные попытки взлома компьютерных систем или сетей с целью кражи данных, нарушения работы или нанесения ущерба [6,7].

Вредоносное ПО (Malware) – программы, такие как вирусы, трояны, шпионское ПО, предназначенные для кражи или уничтожения информации.

Фишинг – метод социальной инженерии, при котором злоумышленники выманивают конфиденциальные данные, маскируясь под доверенные источники.

Атаки типа «человек посередине» (MITM) – перехват данных между пользователем и системой, позволяющий атакующему изменять или похищать информацию.

DDoS-атаки – перегрузка систем огромным количеством запросов, приводящая к их выходу из строя.

Утечки данных – несанкционированный доступ или потеря конфиденциальной информации, что может привести к финансовым и репутационным потерям.

Способы защиты от киберугроз — это метод или набор мер, направленных на предотвращение, обнаружение и устранение угроз, возникающих в цифровой среде. Киберугрозы могут включать в себя вирусы, хакерские атаки, утечку данных, фишинг, вредоносные программы и другие формы угроз, которые могут повредить компьютерные системы, сети или данные. Способы защиты обеспечивают безопасность информации, предотвращают её утрату или повреждение и помогают минимизировать последствия атак. Для эффективной защиты от кибератак необходимо применять комплексные меры безопасности, включающие технологические и организационные решения:

Криптография и шифрование – использование алгоритмов шифрования для защиты данных от несанкционированного доступа [8,9].

Двухфакторная аутентификация (2FA) – дополнительный уровень защиты, требующий подтверждения личности через второй фактор (SMS-код, биометрия и др.).

Антивирусное программное обеспечение – инструменты, выявляющие и блокирующие вредоносные программы.

Фильтрация и защита электронной почты – предотвращение фишинговых атак с помощью автоматизированных фильтров.

Мониторинг и анализ трафика – выявление аномального поведения в сети для предотвращения угроз.

Обучение сотрудников – повышение осведомленности пользователей о киберугрозах и безопасном поведении в интернете.

Регулярное обновление ПО – устранение уязвимостей путем своевременной установки обновлений и патчей безопасности.

Резервное копирование данных – создание бэкапов для восстановления информации в случае кибератаки.

Роль государства и бизнеса в обеспечении кибербезопасности: государственные структуры и бизнес-организации должны активно участвовать в защите данных и информационных систем. Важные аспекты:

Разработка и внедрение законодательных норм, регулирующих сферу кибербезопасности.

Создание национальных центров кибербезопасности для мониторинга угроз и оперативного реагирования.

Взаимодействие государственных и частных организаций для обмена данными о кибератаках [2,10].

Внедрение стандартов и сертификаций для обеспечения защиты информационных систем.

Заключение: В условиях стремительной цифровизации кибербезопасность играет ключевую роль в защите данных, финансов и личной информации. Эффективное противодействие киберугрозам требует комплексного подхода, включающего технологические решения, организационные меры и активное участие государственных и бизнес-структур. Только совместными усилиями можно создать безопасную цифровую среду и минимизировать риски, связанные с киберугрозами [3,11].

Список литературы:

1. Ibragimov, Z. Z. (2022). Application of the Nettest Network Testing Software Package on the Lessons Information Technology. *The Peerian Journal*, *10*, 14-16.

2. Искандарова, З. А. (2021). Сферы применения искусственного интеллекта в работе по управлению персоналом. In *Инновационные подходы в современной науке* (pp. 23-27).
3. Yuldashev, F., & Bobur, U. (2020). Types of Electrical Machine Current Converters. *International Journal of Engineering and Information Systems (IJEAIS) ISSN*, 162-164.
4. Ibragimov, Z., & Ibragimova, N. (2021). Информационные технологии в сфере туризма в Узбекистане. *Boshlang'ich ta'limda innovatsiyalar*, *2*(2).
5. Бегматова, Н. З. (2020). Загрязнение и охрана окружающей среды. Причины и последствия. *Символ науки*, (6), 19-21.
6. Ибрагимова, Н. А., & Ибрагимов, З. З. (2020). Анализ этапа программирования для определения погрешностей процесса обработки деталей с числовым программным управлением. *Энигма*, (25), 137-142.
7. Ubaydullayevich, B. A. (2024). Kredit-modul talim tizimida mustaqil talimning dolzarb muammolari.
8. Ибрагимов, З. З., & Ибрагимова, Н. А. (2020). Обзор методов трехмерного сканирования. *Энигма*, (27-3), 191-194.
9. Аллаберганова, Г. М., Кутбеддинов, А. К., Каримов, А. М., & Кудратов, Э. А. (2015). Интерактивные методы обучения студентов естественных специальностей на основании радиационных факторов экосистемы. *Педагогика и современность*,1,39-43.
10. Абдиев, Х., Умаров, Б., & Тоштемиров, Д. (2021). Структура и принципы солнечных коллекторов. In *наука и современное общество: актуальные вопросы, достижения и инновации* (pp. 9-13).
11. Ибрагимова, Н. А., & Ибрагимов, З. З. (2021). Платформа moodle–необходимый инструмент для преподователей. *Academic research in educational sciences*, *2*(CSPI conference 1), 572-575.