

УДК 62

Аманова А.

Преподаватель

Туркменский государственный архитектурно-строительный институт,

Туркменистан, г. Ашхабад

Чарыева К.

Преподаватель

Туркменский государственный архитектурно-строительный институт,

Туркменистан, г. Ашхабад

Дурдымаммедов Г.

Студент

Туркменский государственный архитектурно-строительный институт,

Туркменистан, г. Ашхабад

УГРОЗЫ ЦИФРОВОГО БУДУЩЕГО

Аннотация

Кибербезопасность становится критически важным аспектом современного цифрового общества. В статье рассматриваются ключевые проблемы в области кибербезопасности, включая угрозы, связанные с развитием Интернета вещей (IoT), искусственного интеллекта (ИИ) и облачных технологий. Анализируются перспективные решения, такие как применение блокчейна, развитие квантовой криптографии и использование технологий машинного обучения для предотвращения атак.

Ключевые слова:

кибербезопасность, интернет вещей, искусственный интеллект, блокчейн, квантовая криптография, цифровая безопасность, машинное обучение.

Цифровизация общества открывает новые горизонты для взаимодействия, автоматизации и экономического роста. Однако с увеличением количества подключенных устройств и ростом объемов данных возрастает и уязвимость киберпространства. Кибератаки становятся всё более сложными, нанося ущерб государственным, корпоративным и личным интересам.

Интернет вещей объединяет миллиарды устройств, от умных холодильников до промышленных датчиков. Несмотря на удобство, IoT представляет собой серьёзную угрозу безопасности из-за низкого уровня защищенности большинства устройств. Атаки, подобные Mirai Botnet в 2016 году, демонстрируют, как легко IoT-устройства могут быть использованы для масштабных кибератак.

ИИ активно применяется хакерами для создания более эффективных методов атак, таких как автоматическое обнаружение уязвимостей и написание вредоносного кода. Например, ИИ может использоваться для запуска фишинговых кампаний с персонализированным подходом, что увеличивает их эффективность.

С переходом бизнеса и государственных служб на облачные платформы возникают новые риски. Потенциальные утечки данных и компрометация облачных систем угрожают конфиденциальности и целостности информации.

Блокчейн, будучи распределённой и неизменяемой технологией, может обеспечить высокий уровень защиты данных. В частности, он эффективен для защиты транзакций, предотвращения подделки данных и создания безопасных систем аутентификации.

С развитием квантовых компьютеров традиционные методы шифрования становятся уязвимыми. Квантовая криптография предлагает решения, основанные на принципах квантовой физики, которые практически невозможно взломать, обеспечивая безопасность данных в долгосрочной перспективе.

Системы на основе машинного обучения способны анализировать огромные массивы данных в реальном времени, идентифицируя аномалии и предотвращая потенциальные атаки. Такие решения активно применяются для защиты финансовых транзакций и обнаружения вредоносной активности в сетях.

С развитием технологий кибербезопасности необходимо учитывать их возможное использование для нарушения прав человека. Например, технологии слежения и анализа данных могут угрожать конфиденциальности пользователей. Государства и международные организации должны разрабатывать согласованные стандарты и законы, обеспечивающие баланс между безопасностью и правами человека.

Кибербезопасность будущего будет основываться на интеграции различных технологий. Коллаборация между правительствами, компаниями и научными учреждениями станет ключевым фактором успеха. Развитие технологий, таких как квантовые сети и самообучающиеся системы защиты, позволит противостоять растущим угрозам.

Кибербезопасность — это не просто защита данных, а основа для стабильного развития цифрового общества. Только через инвестиции в инновации, сотрудничество и создание новых стандартов можно обеспечить безопасное будущее для всех.

Список использованной литературы:

1. Котлер, Ф., Скотт, Д. Цифровая трансформация: как использовать современные технологии для конкурентных преимуществ. — М.: Альпина Паблишер, 2020. — 256 с.
2. Национальная программа "Цифровая экономика Российской Федерации". Официальный сайт Министерства цифрового развития. URL: <https://digital.gov.ru> (дата обращения: 17.11.2024).
3. Росс, А. Индустрия будущего: как технологии изменят мир. — М.: Манн, Иванов и Фербер, 2021. — 304 с.
4. Портер, М. Э. Конкурентное преимущество в цифровую эпоху: стратегические вызовы и возможности // Журнал стратегических исследований. — 2021. — №5. — С. 22–29.

© Аманова А., Чарыева К., Дурдымаммедов Г., 2024

УДК 1082

Аннанепесов Б.О.

Преподаватель

Туркменская государственная детская музыкальная школа имени Данатара Овезова
рядом с Туркменской национальной консерваторией имени Майи Кулиевой

Солтанова Г.

Преподаватель

Джумаев Д.

Преподаватель

Хайытов М.

Преподаватель

Научный Руководитель: Исмаилов Б.

Преподаватель Института инженерно-технических
и транспортных коммуникаций Туркменистана,
Г. Ашхабад Туркменистан

ОСНОВНЫЕ ПРИНЦИПЫ НАУЧНО-ТЕХНИЧЕСКОЙ ПОЛИТИКИ 2

Актуальные вопросы технологического развития научно-технической политики Туркменистана