Тихонова Юлия Максимовна
студентка
Научный руководитель
Сомова Марина Валериевна
доцент

Институт космических и информационных технологий
ФГАОУ ВО «Сибирский федеральный университет»
г. Красноярск, Красноярский край

ЭВОЛЮЦИЯ КИБЕРУГРОЗ: НОВЫЕ ТРЕНДЫ И СТРАТЕГИИ ЗАЩИТЫ

Аннотация: *в работе исследуются преобразования природы современных киберугроз, вызванные цифровизацией общества и широкими технологиями распределённых вычислений, облачных сервисов, интернета вещей и искусственного интеллекта. Отмечается существенное изменение характеристик атак: от точечных вирусных нарушений и локальных вторжений к сложно устроенным, долгосрочным и адаптивным кампаниям. Рассматриваются современные подходы к построению безопасной архитектуры.*

Ключевые слова*: киберугрозы, информационная безопасность, deepfake, социальная инженерия, APT, цифровая трансформация, искусственный интеллект.*

Цифровая трансформация общества, сопровождающаяся повсеместным распространением облачных сервисов, интернета вещей (IoT) и искусственного интеллекта (ИИ), существенно меняет природу современных киберугроз. Вместо точечных атак современные угрозы становятся сложными, гибкими и адаптивными. Традиционные вирусы уступают место крупномасштабным кампаниям: APT, атакам на цепочки поставок, deepfake и социальной инженерии. Наблюдается рост количества инцидентов и усложнение преступлений благодаря использованию машинного обучения, автоматизации и анализа поведения. Это делает устаревшими традиционные подходы к обеспечению информационной безопасности.

Как отмечается в работе [1], за последние десятилетия масштабы и сложность кибератак возросли многократно: ранее защита строилась против стандартных угроз вроде троянов и сетевых червей, однако развитие глобальной сети и усиление взаимозависимости информационных инфраструктур привели к возникновению гораздо более сложных атак нового поколения.

Современные угрозы характеризуются применением ИИ, deepfake, атаками на облака и IoT, фишингом и утечками данных. Исследование [2] выделяет ключевые направления эволюции угроз: рост атак на облачные сервисы, активизация социальной инженерии и применение ИИ.

Современный ландшафт киберугроз характеризуется глубокой трансформацией, приобретающей гибридный и адаптивный характер, интегрируя технические и социально-инженерные аспекты. Исследования показывают, что переход к цифровой экономике и широкое внедрение технологий распределённых вычислений (облачные сервисы, Интернет вещей (*IoT*), 5G-инфраструктура) обусловили появление новых классов угроз, ранее отсутствовавших в классических IT-системах [3].

Отдельное направление исследований представлено в работе [4], где подчеркивается смена вектора нападения с технических компонентов на человеческие факторы. Пользовательская активность стала основной точкой риска, особенно в свете увеличения практики дистанционной работы и политики *Bring Your Own Device* (*BYOD)*

Возрастающая сложность и разнообразие современных киберугроз вынуждает организации переходить к архитектуре информационной безопасности, которая способна защищать не только отдельные ресурсы и точки доступа, но и саму структуру корпоративной сети. Одним из эффективных направлений решения данной проблемы выступает концепция архитектуры нулевого доверия (*Zero Trust Architecture, ZTA).*

В статье [5] подробно рассмотрена реализация концепции *Zero Trust* применительно к промышленному сегменту Интернета вещей (*IoT*). Подчёркивается, что традиционные средства защиты оказываются недостаточными в

высокораспределённых, разнородных и чувствительных к временным задержкам системах, таких как промышленные *IoT*-сети.

Принцип *Zero Trust* в сочетании с сегментированной структурой сети, развитыми механизмами идентификации и контроля доступа, а также возможностями программно-определяемой инфраструктуры позволяют построить надежную систему защиты.

Таким образом, работа подчёркивает трансформацию киберугроз в условиях цифровизации и необходимость перехода от традиционных моделей безопасности к адаптивным, ориентированным на проактивное реагирование и устойчивость систем. Особое внимание уделяется таким аспектам, как использование искусственного интеллекта в атаках, рост роли социальной инженерии и уязвимости цепочек поставок.

Список литературы

1. Cybersecurity: State of the Art, Challenges and Future Directions. – Elsevier, 2020.

2. Forecasting Cyber Threats and Pertinent Mitigation Technologies. – Elsevier, 2021.

3. A comprehensive review study of cyber-attacks and cyber security // Emerging trends and recent developments. – Elsevier, 2021.

4. Unraveling the Dynamics of the Cyber Threat Landscape: Major Shifts and Emerging Patterns. – Elsevier, 2024.

5. Zanasi C. Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures / C. Zanasi, S. Russo // Ad Hoc Networks. – 2024. – №103414. – 156 с. – https://doi.org/10.1016/j.adhoc.2024.103414. – EDN QYWASE