НАУЧНЫЙ ЖУРНАЛ
НАУКА И МИРОВОЗЗРЕНИЕ

УДК-004

АНАЛИЗ УСТОЙЧИВОСТИ ЦИФРОВЫХ ИНФРАСТРУКТУР К КИБЕРАТАКАМ: ВЫЗОВЫ И РЕШЕНИЯ

Калинина Марина Васильевна
Кандидат технических наук, доцент кафедры информационной безопасности
Московский государственный технический университет имени Н.Э. Баумана
г. Москва, Российская Федерация

Ильин Сергей Владимирович
Студент 4 курса факультета информатики и систем управления
Московский государственный технический университет имени Н.Э. Баумана
г. Москва, Российская Федерация

Аннотация

В статье рассматриваются актуальные угрозы, влияющие на устойчивость цифровых инфраструктур к кибератакам. Проанализированы ключевые векторы атак, такие как DDoS, взлом программного обеспечения, фишинг, эксплуатация уязвимостей и атаки с использованием искусственного интеллекта. Особое внимание уделено механизмам повышения устойчивости: созданию резервных систем, применению средств криптографической защиты, технологии Zero Trust и обучению персонала. Представлены как теоретические основы, так и практические примеры из реальной кибербезопасности. Предложены рекомендации по повышению устойчивости ИТ-инфраструктур в условиях современных угроз.

Ключевые слова: кибератаки, цифровая инфраструктура, информационная безопасность, DDoS, Zero Trust, устойчивость, киберугрозы, киберзащита

1. Введение

Цифровая инфраструктура стала неотъемлемой частью функционирования современного общества, включая энергетику, транспорт, здравоохранение, образование и госуправление. Однако рост цифровизации привёл и к росту киберугроз. Атаки на критически важные ИТ-объекты способны парализовать целые сектора экономики, нарушить социальную стабильность и нанести колоссальный ущерб.

Устойчивость цифровых систем — это их способность сохранять работоспособность и защищённость в условиях воздействия различных деструктивных факторов, включая внешние кибератаки.

Поэтому вопрос устойчивости становится центральным в политике кибербезопасности государства и бизнеса.

2. Основные векторы кибератак

2.1 DDoS-атаки

Атаки типа Distributed Denial of Service направлены на перегрузку сетевых ресурсов. Их цели — вывести из строя веб-сервисы, нарушить работу приложений и коммуникаций. Сложность борьбы заключается в том, что атака идёт из распределённых источников (ботнетов), часто с использованием IoT-устройств.

2.2 Вредоносное ПО и эксплойты

Хакеры используют трояны, шифровальщики и черви для получения доступа к системам, похищения данных или их уничтожения. Часто вредоносный код распространяется через фишинговые письма или скрывается в обновлениях программ.

2.3 Социальная инженерия и фишинг

Человеческий фактор остаётся самой уязвимой частью ИТ-систем. Злоумышленники манипулируют сотрудниками компаний, заставляя их раскрывать пароли или устанавливать вредоносные программы.

2.4 Целевые атаки и APT

Advanced Persistent Threats — атаки, направленные на длительное скрытное присутствие в инфраструктуре с целью промышленного шпионажа или саботажа. Используются в кибервойнах и против стратегических объектов.

3. Оценка устойчивости цифровой инфраструктуры

Анализ устойчивости включает:

- **Аудит ИТ-активов** — инвентаризация всех компонентов системы, включая аппаратное обеспечение, сети и ПО.
- **Оценка уязвимостей** — с использованием сканеров (например, Nessus, OpenVAS).
- **Тестирование на проникновение (pentest)** — моделирование кибератак с целью выявления слабых мест.
- **Анализ резервного копирования** — проверка частоты, надёжности и независимости копий данных.

Пример: исследование компании IBM показало, что компании, проводившие регулярное тестирование на проникновение, снижали риск серьёзного инцидента на 58%.

4. Современные решения и подходы

4.1 Архитектура Zero Trust

Подход Zero Trust («ноль доверия») предполагает, что **ни один пользователь или устройство не считаются доверенными по умолчанию**, даже находясь внутри периметра сети. Основные принципы:

- верификация на каждом этапе;
- минимальные привилегии;
- микросегментация сети.

Это позволяет ограничить движение злоумышленника внутри инфраструктуры при успешной атаке.

4.2 Резервирование и избыточность

Создание **отказоустойчивых систем** с резервными каналами связи, дублированием серверов, регулярным созданием backup'ов — основа технологической устойчивости. Важны также offline-копии данных, защищённые от сетевого воздействия.

4.3 Криптографическая защита

Использование современных алгоритмов шифрования (AES, RSA, ECC), цифровых подписей, блокчейна и инфраструктуры открытых ключей (PKI) обеспечивает конфиденциальность, целостность и аутентичность информации.

4.4 Мониторинг и SIEM-системы

Security Information and Event Management (SIEM) — автоматический анализ событий безопасности. Позволяет:

- выявлять аномалии;
- оповещать о вторжениях в режиме реального времени;
- ускорять реагирование на инциденты.

Популярные решения: Splunk, QRadar, ArcSight.

4.5 Подготовка персонала

Обучение сотрудников основам кибергигиены, проведение фишинговых симуляций и тренингов существенно снижает уязвимость систем. По данным Verizon, более 80% успешных атак начинались с фишинга.

5. Примеры атак и уроки

- **Атака на Colonial Pipeline (США, 2021)** — привела к остановке крупнейшего нефтепровода. Причина: утечка пароля VPN и отсутствие двухфакторной аутентификации.
- **SolarWinds (2020)** — масштабная цепная атака, затронувшая госструктуры США. Вредоносный код был внедрён в обновления популярного ПО.
- **NotPetya (2017)** — кибератака, ориентированная на инфраструктуру Украины, распространившаяся глобально, нарушив работу транспортных и логистических компаний.

Уроки: критически важна многоуровневая защита и отслеживание изменений в инфраструктуре.

Заключение

Устойчивость цифровой инфраструктуры в условиях нарастающих киберугроз становится краеугольным камнем национальной безопасности и бизнес-устойчивости. Не существует универсального решения — необходим комплексный подход, включающий как технические меры (Zero Trust, шифрование, SIEM), так и человеческий фактор (обучение, контроль доступа). Только сочетание стратегического планирования, регулярной оценки уязвимостей и внедрения инновационных подходов позволяет создать по-настоящему устойчивую ИТ-среду. В условиях геополитической турбулентности и цифровых трансформаций эта задача приобретает первостепенное значение.

Литература

1. IBM X-Force Threat Intelligence Report, 2023.
2. National Institute of Standards and Technology (NIST). Special Publication 800-207: Zero Trust Architecture.
3. Schneier B. *Secrets and Lies: Digital Security in a Networked World*. Wiley, 2015.
4. Павлов И.А., Ильин С.В. Архитектура Zero Trust: теория и практика. // Вестник МГТУ им. Баумана. – 2023.
5. Cisco Systems. *Cybersecurity Threat Trends Report*. 2024.
6. Verizon Data Breach Investigations Report (DBIR), 2024.