DOI 10.37539/2949-1991.2023.9.9.012
УДК 004.056

Шабалин Иван Николаевич, студент
кафедры «Безопасность информационных систем»
Нижегородский государственный университет им. Н.И. Лобачевского, Нижний Новгород, Россия

Никитин Артем Владимирович, студент
кафедры «Безопасность информационных систем»
Нижегородский государственный университет им. Н.И. Лобачевского, Нижний Новгород, Россия

Коротышева Анна Андреевна, аспирант
кафедры «Безопасность информационных систем»
Нижегородский государственный университет им. Н.И. Лобачевского, Нижний Новгород, Россия

АНАЛИЗ СОВРЕМЕННЫХ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Аннотация. В статье представлен обзор основных угроз и уязвимостей, которые сейчас существуют в области информационной безопасности. Рассмотрены технологии и методы, разработанные для обеспечения целостности, конфиденциальности и доступности данных в условиях растущих угроз со стороны хакеров, киберпреступников и государственных хакерских групп.

Ключевые слова: информационная безопасность, защита информации, компьютерная атака, метод защиты информационной инфраструктуры, машинное обучение.

Введение

Современная информационная эпоха сопровождается внушительным ростом технологических возможностей, но также и угроз безопасности, влияющими на организации и частных пользователей по всему миру. Число кибератак в РФ в первом квартале 2023 года выросло в полтора раза в сравнении с аналогичным периодом 2022 года, до 290 тыс. [1]. При этом 56% высококритичных инцидентов связано с применением вредоносного софта, 9% - с использованием нелегитимного программного обеспечения (ПО). Долю в 8% составили сетевые атаки, 7% инцидентов связано с эксплуатацией уязвимостей, еще 6% - с несанкционированным доступом, 4% - с компрометацией учетных записей, следует из отчета.

Угрозы в области информационной безопасности

Рассмотрим некоторые из основных угроз и уязвимостей, с которыми мы сталкиваемся в настоящее время:

1. Кибератаки и хакерские атаки:

- DDoS-атаки (Distributed Denial of Service): нападение, целью которого является перегрузка веб-сайта или онлайн-сервиса, делая его недоступным для легальных пользователей.
- Малициозное ПО: вирусы, троянские программы, шпионское ПО и зловредное ПО (англ. Ransomware), которые могут заражать устройства и красть конфиденциальные данные или шифровать файлы для вымогательства у жертв выкупа [2].

2. Фишинг:

- Направленный фишинг (англ. Spear Phishing): хакеры маскируются под доверенные источники, чтобы получить доступ к конфиденциальным данным, часто путем манипуляции сотрудниками компании.

3. Утечки данных и нарушение конфиденциальности:

- Утечки персональных данных: атаки на базы данных огромных организаций, в результате чего персональные данные миллионов пользователей могут оказываются в руках злоумышленников.

- Нарушение конфиденциальности в облачных сервисах: утечки данных из облачных хранилищ, что может привести к несанкционированному доступу к чувствительной информации [3].

4. Недостаточная защита IoT (Интернет вещей):

- Неустранимые уязвимости в устройствах: множество IoT-устройств не обладают должным уровнем безопасности, что делает их уязвимыми для атак [4].

5. Угрозы искусственного интеллекта (ИИ) и машинного обучения (МО):

- Deepfake: манипуляция медиа-контентом с использованием ИИ, что может привести к распространению фальшивой информации.

- Вредоносное МО (англ. Adversarial Machine Learning): манипулирование данными для обучения моделей, атаки на модели МО [5].

6. Недостатки в кибергигиене и обучении пользователей:

- Слабые пароли и недостаточная аутентификация: многие пользователи используют слабые пароли или используют один пароль для нескольких сервисов.

- Нежелание пользователей обучаться: многие пользователи не знают основ безопасности или не проявляют интерес к обучению, что делает их более подверженными атакам.

7. Государственные кибератаки:

- Шпионаж: государства и киберпреступные группы могут вмешиваться в информационные системы других стран для получения конфиденциальных данных.

- Кибервоенные действия: возможность кибератак для отключения критической инфраструктуры других стран.

Борьба с этими угрозами требует постоянного обновления и совершенствования технологических решений, обучения пользователей и развития международного сотрудничества для эффективного обмена информацией о киберугрозах и методах их предотвращения.

Методы защиты информационных систем

Современные методы защиты информационных систем становятся все более сложными и инновационными, чтобы справиться с угрозами в постоянно меняющемся киберландшафте. Рассмотрим ключевые методы, которые играют важную роль в современной кибербезопасности:

1. Криптография нового поколения:

- Квантовая криптография [6]: использует принципы квантовой механики для создания систем, которые невозможно взломать с использованием классических криптографических методов дешифровки.

- Многозначные криптосистемы: исследования в области криптографии с многозначными функциями позволяют создавать более устойчивые к атакам системы шифрования.

2. Искусственный интеллект и машинное обучение:

- Анализ поведения: ИИ и МО используются для выявления необычных или подозрительных активностей, что помогает выявлять атаки на основе аномалий в поведении пользователей и систем.

- Прогнозирование атак: алгоритмы МО позволяют предсказывать вероятные угрозы, а также определять наиболее подходящие стратегии для предотвращения атак.

3. Блокчейн:

- Децентрализация и непреложность данных: блокчейн обеспечивает децентрализованное хранение данных, что делает сложным их модификацию или взлом.

- Умные контракты: позволяют создавать автоматизированные контракты, основанные на блокчейне, что снижает риск мошенничества и обеспечивает безопасные транзакции.

4. Методы обнаружения и предотвращения атак:

- Анализ поведения системы: мониторинг и анализ поведения системы позволяют выявлять необычные активности, которые могут свидетельствовать о кибератаках [7].

- Сетевые механизмы безопасности: использование сетевых брандмауэров, интранет-сегментации и систем обнаружения вторжений помогает в создании многоуровневой защиты от различных видов атак.

5. Анализ угроз и интеллектуальная безопасность:

- Углубленный анализ угроз: применение искусственного интеллекта для анализа больших данных об угрозах, что позволяет идентифицировать новые угрозы и создавать более эффективные методы их предотвращения.

- Интеллектуальная безопасность: использование технологий искусственного интеллекта для выявления и предотвращения утечек данных, а также защиты интеллектуальной собственности компаний.

Эти методы являются лишь частью непрерывно развивающегося ландшафта угроз кибербезопасности. Интеграция этих инновационных технологий и методов в информационные системы помогает создать более устойчивые и защищенные от атак среды, обеспечивая безопасность как организаций, так и частных лиц.

Заключение

Таким образом, внедрение и постоянное совершенствование современных методов защиты информации позволит динамически адаптироваться к появлению новых видов киберугроз.

Список литературы:

1. В России в первом квартале 2023 года число кибератак выросло до 290 тыс. [Электронный ресурс]. – Режим доступа: https://tass.ru/ekonomika/17610537. – (Дата обращения: 12.10.2023).

2. Young A. and Yung M. Cryptovirology: extortion-based security threats and countermeasures // Proceedings 1996 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 1996, pp. 129-140. DOI:10.1109/SECPRI.1996.502676.

3. Ширманов А. Безопасность виртуализации при обработке данных ограниченного доступа // Москва, ЭКСПОЦЕНТР, InfoSecurity Russia (30 сентября 2009).

4. Наралиев Н.А., Самаль Д.И. Обзор и анализ стандартов и протоколов в области интернет вещей. Современные методы тестирования и проблемы информационной безопасности IoT // International Journal of Open Information Technologies. – 2019. – №8.

5. Ласков, П., Липпманн, Р. Машинное обучение в состязательной среде // Машинное обучение. – 2010. – 81 (2). – С. 115–119. DOI:10.1007/s10994-010-5207-6.

6. Долгочуб Е.А., Поликанин А.Н. Технологии квантовой криптографии // Интерэкспо Гео-Сибирь. – 2021. – №. 6. – С. 78-83. DOI:10.33764/2618-981X-2021-6-78-83.

7. Очередько А.Р. [и др.] Исследование SIEM-систем на основе анализа механизмов выявления кибератак // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. – 2020. – №. 2 (261). – С. 25-31.