Охотин Данил Александрович,
Студент, Краснодар

Акишин Андрей Владимирович,
Доцент, Краснодар

Хечиев Наран Валерьевич
Студент**,** Краснодар

Свистун Никита Сергеевич
Студент, Краснодар

Кубенко Егор Георгеевич
старший преподаватель, Краснодар

Ковнацкий Маким Феликсович
Слушатель, Краснодар

АНАЛИЗ И КЛАССИФИКАЦИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Аннотация: В статье проведен анализ и классификация угроз информационной безопасности автоматизированных систем. Представлена классификация, основанная на различных критериях, что позволяет систематизировать знания об угрозах и является основой для разработки эффективных мер защиты. Результаты исследования могут быть использованы в практической деятельности специалистов по информационной безопасности.

Ключевые слова: угроза информационной безопасности, автоматизированные системы, информационная безопасность,

Термины и определения:

1. Угроза информационной безопасности Российской Федерации (далее – информационная угроза) – совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере [1].

2. Автоматизированная система (АС) – это система, состоящая из комплекса средств автоматизации, реализующего информационную технологию выполнения установленных функций, и персонала, обеспечивающего его функционирование [2].

Введение. В условиях возрастающей зависимости от автоматизированных систем (АС), проблема обеспечения их информационной безопасности становится все более актуальной. Многообразие потенциальных угроз, их сложность и потенциальные последствия требуют глубокого анализа и систематизации. В рамках данной статьи мы стремимся провести всесторонний анализ существующих и потенциальных угроз, направленных на АС. Цель работы заключается в разработке классификации угроз, которая может быть использована специалистами в области информационной безопасности для разработки более эффективных мер по предотвращению и нейтрализации кибератак на автоматизированные системы.

Обзор основных типов угроз для автоматизированных систем:

1.1. Внешние угрозы – это угрозы, исходящие извне, от внешних злоумышленников и киберпреступников.

Типы угроз:

1. Сетевые атаки:

- DDoS-атаки (распределенный отказ в обслуживании);

- Сканирование портов и уязвимостей;
- MITM-атаки (Man-in-the-Middle);
- Внедрение вредоносного кода через сеть [3].

2. Фишинг и социальная инженерия:
- Манипулирование персоналом для получения доступа системам;
- Фишинговые электронные письма и веб-сайты.

3. Вредоносное программное обеспечение (ПО):
– Вирусы, черви, трояны;
– Программы-вымогатели (Ransomware);
– Шпионское ПО.

1.2. Внутренние угрозы – это угрозы, исходящие от персонала организации, как преднамеренные, так и непреднамеренные.

Типы угроз:

1. Несанкционированный доступ:
– Злоупотребление полномочиями доступа;
– Случайный или преднамеренный доступ к конфиденциальной информации;
– Человеческий фактор (ошибки и небрежность):
• Неправильная конфигурация систем;
• Несвоевременное обновление программного обеспечения;
• Потеря или кража учетных данных.

2. Саботаж – это преднамеренные действия по нанесению ущерба системе

1.3. Угрозы, связанные с уязвимостями – это уязвимости в программном обеспечении, конфигурации и архитектуре АС, которые могут быть использованы злоумышленниками.

Типы угроз:

– Уязвимости “нулевого дня” (неизвестные уязвимости, для которых еще не существует патчей);
– Устаревшее ПО (использование ПО с известными уязвимостями);
– Неправильные настройки (некорректно настроенные брандмауэры, службы и приложения);
– Слабые пароли (использование простых или стандартных паролей);

2. Характеристики угроз информационной безопасности:

2.1. По источнику:
– Внешние (киберпреступники, конкуренты);
– Внутренние (сотрудники, подрядчики).

2.2. По цели:
– Кража данных;
– Нарушение целостности данных;
– Нарушение доступности (отказ в обслуживании);
– Получение несанкционированного доступа;
– Шпионаж и саботаж [3].

2.3. По уровню угрозы:
- Низкий;
- Средний;
- Высокий.

2.4. По способу реализации:
– Активные (прямые атаки);
– Пассивные (перехват информации).

2.5. По вектору атаки:
– Сетевые;
– Почтовые;
– Физический доступ;
– Уязвимости ПО.

3. Анализ потенциальных последствий угроз:
3.1. Финансовые потери:
– Ущерб от простоя системы;
– Ущерб от потери данных;
– Расходы на восстановление системы;
– Уплата штрафов и судебные издержки.
3.2. Репутационные потери:
– Утрата доверия клиентов;
– Негативный имидж организации.
3.3. Нарушение функционирования АС:
– Сбои в работе системы [3].
– Недоступность сервисов
– Утрата контроля над системой
3.4. Угроза безопасности людей – воздействие на критически важную инфраструктуру (энергетика, транспорт, медицина)

Проведенный анализ угроз информационной безопасности, нацеленных на автоматизированные системы, показывает их многообразие, сложность и потенциальную опасность. Для эффективной защиты АС необходимо учитывать все возможные типы угроз, их характеристики и потенциальные последствия. В следующем разделе статьи мы рассмотрим различные подходы к классификации этих угроз, что позволит систематизировать знания и облегчить процесс принятия решений по обеспечению информационной безопасности.

Данный анализ будет проводится как по существующим автоматизированным системам так и по специальному программному обеспечению, такому как «Специальное программное обеспечение автоматизации контроля за событиями информационной безопасности» [4].

Анализ угроз:

1. DDoS-атаки (Distributed Denial of Service):

– По данным отчета Kaspersky DDoS Attacks in Q1 2024:

количество DDoS-атак в первом квартале 2024 года возросло на 20% по сравнению с аналогичным периодом прошлого года [5].

– По оценкам экспертов, средняя продолжительность

DDoS-атаки на АС составляет от 12 до 24 часов, а максимальная может достигать нескольких суток [6].

– Средний ущерб от успешной DDoS-атаки на крупное предприятие, по данным Ponemon Institute, может варьироваться от 100 000 до 500 000 долларов США [7].

2. Вредоносное программное обеспечение (ПО):

- По данным Check Point Software Technologies, количество атак с использованием программ-вымогателей (ransomware) в 2023 году увеличилось на 30% по сравнению с предыдущим годом [8].

- В 2023 году было зафиксировано более 10 миллионов случаев заражения вредоносным ПО через электронную почту [9].

- Средний ущерб от атаки с использованием ransomware, по данным Coveware, составляет около 1,85 миллиона долларов США [10].

3. Атаки с использованием социальной инженерии:

- Согласно отчетам Verizon Data Breach Investigations Report, 82% утечек данных связаны с человеческим фактором и ошибками персонала [11].

- Более 60% атак с использованием ransomware начинаются с фишинговых электронных писем [12].

- Средний ущерб от утечки данных в результате социальной инженерии составляет от 100 000 до 1 000 000 долларов США [13].

Вывод

Проведенный анализ угроз информационной безопасности на автоматизированных системах с использованием статистических данных, отчетов и примеров, подчеркивает серьезность проблемы и необходимость принятия эффективных мер защиты. Наиболее распространенными угрозами являются DDoS-атаки, вредоносное ПО, атаки с использованием социальной инженерии и эксплуатация уязвимостей. Каждая из этих угроз требует особого внимания и комплексного подхода к защите.

Список литературы:

1.Доктрина информационной безопасности Российской Федерации, утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646.

2. ГОСТ Р 59853-2021 "Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения" утвержден приказом Росстандарта от 19 ноября 2021 г. № 1520-ст

3. Иванов, К. К. Угрозы безопасности информации в автоматизированных системах / К. К. Иванов, Р. Н. Юрченко, А. С. Ярмонов. – Текст: непосредственный // Молодой ученый. – 2016. – № 29 (133). – С. 20-22. – URL: https://moluch.ru/archive/133/37181/ (дата обращения: 19.01.2025).

4. Свидетельство о государственной регистрации программы для ЭВМ № 2024617023 Российская Федерация. Специальное программное обеспечение автоматизации контроля за событиями информационной безопасности: № 2024615656: заявл. 19.03.2024: опубл. 27.03.2024 / А. М. Бородин, Н. Н. Енин, А. Е. Углов [и др.]. – EDN NAOVXO.

5. DDoS-атаки «Лаборатории Касперского» в Q1 2024 [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru

6. Экспертная оценка компаний в области кибербезопасности [Электронный ресурс]. – Режим доступа: https:// ir.alfastrah.ru

7. Ponemon Institute [Электронный ресурс]. – Режим доступа: https:// ponemon.org

8. Check Point Software Technologies [Электронный ресурс]. – Режим доступа: https:// checkpoint.com

9. Статистика по вредоносному ПО из открытых источников [Электронный ресурс]. – Режим доступа https://www.kaspersky.ru

10. Coveware [Электронный ресурс]. – Режим доступа: https:// coveware.com

11. Verizon Data Breach Investigations Report [Электронный ресурс]. – Режим доступа: https:// newsletter.radensa.ru

12. Статистика по фишингу из открытых источников [Электронный ресурс]. – Режим доступа https:// securelist.ru

13. Оценка ущерба от утечек данных из открытых источников: [Электронный ресурс]. – Режим доступа https:// infowatch.ru