Федеральное государственное автономное образовательное учреждение
высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий
Кафедра «Информационная безопасность»

Направление подготовки: 10.05.03 Информационная безопасность автоматизированных систем

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

"Анализ инцидентов ИБ в сетевой инфраструктуре и план реагирования"

к отчету

по проектной практике

Студент: Макаренко Анна Ефимовна Группа: 241-372

Место прохождения практики: Московский Политех, кафедра «Информационная безопасность»

Отчет принят с оценкой _____ Дата _____

Руководитель практики: _____

Москва 2025

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В современных условиях развития информационных технологий вопросы информационной безопасности становятся все более актуальными. Сетевая инфраструктура организаций постоянно подвергается различным угрозам, что требует разработки эффективных механизмов обнаружения и реагирования на инциденты ИБ.

Целью данного отчета является анализ инцидентов информационной безопасности в сетевой инфраструктуре и разработка плана реагирования на них.

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Инцидент информационной безопасности – это подтвержденное событие, которое привело или может привести к нарушению политики информационной безопасности организации.

Классификация инцидентов ИБ:

- Несанкционированный доступ
- Вредоносное ПО
- DDoS-атаки
- Социальная инженерия
- Внутренние угрозы
- Физические инциденты
- Технические сбои

Методы обнаружения инцидентов:

- Системы обнаружения вторжений (IDS/IPS)
- Системы мониторинга событий безопасности (SIEM)
- Журналирование и аудит
- Сканирование уязвимостей
- Анализ сетевого трафика

Классификация угроз:

- Атаки на доступность
- Утечки данных

- Внутренние угрозы

Анализ типичных инцидентов:

- Несанкционированное изменение конфигураций сетевых устройств
- Распространение вредоносного ПО через электронную почту
- Компрометация учетных данных
- DDoS-атаки на веб-ресурсы
- Нарушение сегментации сети

Методология расследования инцидентов:

- Обнаружение инцидента
- Оценка серьезности
- Сохранение доказательств
- Анализ причин возникновения
- Устранение последствий
- Документирование инцидента

План реагирования на инциденты:

- Создание группы реагирования
- Разработка процедур уведомления
- Определение приоритетов реагирования
- План восстановления работоспособности
- Обучение персонала
- Проведение учений

Этапы реагирования

1. **Detection**: системы мониторинга (Zabbix, Wazuh)
2. **Analysis**: определение IoC (Indicators of Compromise)
3. **Containment**: сегментация сети, блокировка IP
4. **Eradication**: устранение уязвимостей
5. **Recovery**: восстановление из бэкапов
6. **Lessons Learned**: обновление политик

ПРАКТИЧЕСКАЯ ЧАСТЬ

1. Несанкционированное изменение конфигураций сетевых устройств

Описание инцидента: изменение настроек маршрутизаторов, коммутаторов и файерволов без соответствующего разрешения. Часто происходит через уязвимости в веб-интерфейсах управления или путем компрометации учетных данных администраторов.

Примеры:

- В 2023 году компания Equifax пострадала от атаки, где злоумышленники изменили настройки сетевого оборудования, что позволило им получить доступ к персональным данным миллионов пользователей.
- Атака на сеть Deutsche Telekom, где злоумышленники изменили правила маршрутизации для перехвата трафика.

Методы обнаружения:

- Мониторинг конфигурационных изменений
- Систематическое сравнение текущих настроек с эталонными
- Использование систем контроля версий для конфигураций

2. Распространение вредоносного ПО через электронную почту

Описание инцидента: фишинговые письма с вредоносными вложениями или ссылками на зараженные сайты. Один из самых распространенных векторов атак.

Примеры:

- **WannaCry (2017):** распространение через SMB-протокол и электронные письма, затронуло более 200 000 компьютеров в 150 странах.
- **Emotet (2020):** масштабная кампания, начавшаяся с фишинговых писем, привела к заражению более 1.5 млн устройств.

Методы защиты:

- Антиспам-фильтры
- Санскрининг вложений
- Обучение персонала распознаванию фишинга
- Многофакторная аутентификация

3. Компрометация учетных данных

Описание инцидента: кража или несанкционированное использование учетных данных сотрудников. Часто происходит через методы социальной инженерии или брутфорс-атаки.

Примеры:

- **LinkedIn (2021):** утечка данных 700 млн пользователей, использованная для дальнейших атак.
- **Twitter (2020):** компрометация учетных записей высокопоставленных лиц для проведения фишинговой атаки.

Меры предотвращения:

- Политики сложных паролей
- Регулярная смена паролей
- Мониторинг подозрительной активности

- Использование MFA

4. DDoS-атаки на веб-ресурсы

Описание инцидента: перегрузка серверов легитимным или модифицированным трафиком, приводящая к недоступности сервисов.

Примеры:

- **GitHub (2018):** самая мощная DDoS-атака в истории с пиковой нагрузкой 1.35 Тбит/с.
- **Bank of America (2020):** многодневная DDoS-атака, парализовавшая работу онлайн-сервисов.

Методы защиты:

- Распределенные системы защиты
- Анти-DDoS фильтры
- Балансировка нагрузки
- Резервные каналы связи

5. Нарушение сегментации сети

Описание инцидента: обход механизмов сетевой изоляции, позволяющий злоумышленникам перемещаться по сети.

Примеры:

- **Target (2013):** злоумышленники получили доступ к платежной системе через нарушенную сегментацию сети.
- **Marriott (2018):** атака через нарушенную сегментацию, приведшая к утечке данных 500 млн гостей.

Методы предотвращения:

- Строгая политика сетевого доступа
- Микросегментация
- Мониторинг межсетевого трафика
- Регулярная проверка правил доступа

6. Атаки на цепочку поставок

Описание инцидента: компрометация программного обеспечения через поставщиков или партнеров.

Примеры:

- **SolarWinds (2020):** атака на программное обеспечение SolarWinds Orion, затронувшая тысячи организаций.
- **Kaseya (2021):** атака на программное обеспечение для удаленного управления, затронувшая более 1500 компаний.

Меры защиты:

- Проверка целостности ПО
- Многоуровневая проверка поставщиков
- Мониторинг изменений в программном обеспечении
- Использование систем контроля доступа

7. Эксплуатация нулевого дня

Описание инцидента: использование неизвестных разработчикам уязвимостей для проведения атак.

Примеры:

- **Equation Group (2015):** использование нескольких уязвимостей нулевого дня для проведения кибератак.
- **BlueKeep (2019):** уязвимость в RDP, использованная для распространения вредоносного ПО.

Методы защиты:

- Своевременное обновление ПО
- Использование систем обнаружения вторжений
- Сегментация сети
- Мониторинг подозрительной активност

ПЛАН РЕАГИРОВАНИЯ

1. Подготовительный этап

1.1. Создание группы реагирования (CSIRT)

- Назначение руководителя группы
- Формирование команды специалистов по направлениям:
    - Аналитики безопасности
    - Системные администраторы
    - Сетевые инженеры
    - Юристы
    - PR-специалисты
- Определение ролей и обязанностей каждого члена команды

1.2. Разработка документации

- Регламенты реагирования
- Шаблоны отчетности
- Скрипты действий для типовых инцидентов
- Контакты экстренных служб и регуляторов

1.3. Подготовка инфраструктуры

- Создание изолированной сетевой зоны для расследования
- Резервное хранилище данных
- Системы мониторинга и журналирования
- Средства анализа инцидентов

2. Процедуры обнаружения

2.1. Системы мониторинга

- Настройка SIEM-системы
- Конфигурация IDS/IPS
- Мониторинг журналов событий
- Анализ сетевого трафика

2.2. Каналы получения информации

- Автоматизированные системы оповещения
- Горячая линия для сотрудников
- Внешние источники информации
- Системы сканирования уязвимостей

3. Этапы реагирования

3.1. Обнаружение и оценка

- Фиксация времени обнаружения
- Первичная оценка серьезности
- Определение масштаба инцидента
- Оценка потенциального ущерба

3.2. Изоляция инцидента

- Отключение затронутых систем
- Создание резервных копий
- Блокировка подозрительной активности
- Уведомление ответственных лиц

3.3. Расследование

- Сбор доказательств
- Анализ причин возникновения
- Документирование всех действий
- Оценка ущерба

3.4. Устранение последствий

- Восстановление работоспособности
- Обновление защитных механизмов
- Реализация мер по предотвращению повторения
- Обучение персонала

4. Коммуникация и отчетность

4.1. Внутренние коммуникации

- Оповещение руководства
- Информирование затронутых подразделений
- Координация действий команды
- Ведение журнала событий

4.2. Внешние коммуникации

- Уведомление регуляторов
- Информирование клиентов
- Взаимодействие с правоохранительными органами
- Работа с PR-службами

5. Восстановление и улучшение

5.1. Восстановление систем

- План восстановления
- Тестирование работоспособности
- Проверка безопасности
- Возврат к штатной работе

5.2. Анализ и улучшение

- Пост-инцидентный анализ
- Разработка рекомендаций
- Обновление процедур
- Проведение учений

6. Технические меры реагирования

6.1. Сетевая безопасность

- Настройка правил файервола
- Обновление политик доступа
- Проверка сетевой инфраструктуры
- Мониторинг аномалий

6.2. Защита конечных точек

- Обновление антивирусного ПО
- Сканирование на наличие угроз
- Обновление патчей
- Проверка целостности систем

7. Документация и отчетность

7.1. Обязательная документация

- Журнал инцидентов
- Отчеты о расследовании
- План восстановления
- Протоколы совещаний

7.2. Форма отчетности

- Ежедневные отчеты
- Итоговые отчеты
- Статистические данные

- Рекомендации по улучшению

8. Обучение и тренировки

8.1. Программы обучения

- Регулярные тренинги
- Тематические семинары
- Практические занятия
- Тестирование знаний

8.2. Учения и симуляции

- Плановые учения
- Внезапные тренировки
- Анализ результатов
- Корректировка процедур

9. Интеграция с бизнес-процессами

9.1. Взаимодействие с отделами

- Координация с IT-службой
- Взаимодействие с HR
- Работа с юридическим отделом
- Поддержка бизнес-процессов

9.2. Учет бизнес-рисков

- Оценка влияния на бизнес
- Приоритизация действий

- Минимизация ущерба
- Восстановление ключевых процессов

10. Мониторинг и совершенствование

10.1. Постоянный мониторинг

- Отслеживание эффективности
- Сбор обратной связи
- Анализ инцидентов
- Корректировка процедур

10.2. Развитие системы

- Внедрение новых технологий
- Обновление методик
- Расширение возможностей
- Оптимизация процессов

ЗАКЛЮЧЕНИЕ

В ходе проведенного анализа инцидентов информационной безопаснос ти были рассмотрены основные типы угроз, с которыми сталкиваются сов ременные организации, примеры реальных инцидентов, а также сформирован перечень необходимых технических и организационных мер.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Инциденты: https://www.cert.ru/ru/about.shtml (Дата обращения: 02.05.2025)
2. Меры защиты: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf (Дата обращения: 02.05.2025)
3. Рекомендации по реагированию: https://csrc.nist.gov/pubs/sp/800/61/r3/final (Дата обращения: 02.05.2025)
4. Теория: https://www.microsoft.com/ru-ru/security/business/security-101/what-is-incident-response (Дата обращения: 02.05.2025)
5. https://ics-cert.kaspersky.com/ (Дата обращения: 02.05.2025)