ПРАКТИЧЕСКАЯ РАБОТА

Построение модели угроз на основе методики оценки угроз безопасности информации ФСТЭК от 5.02.2021г.

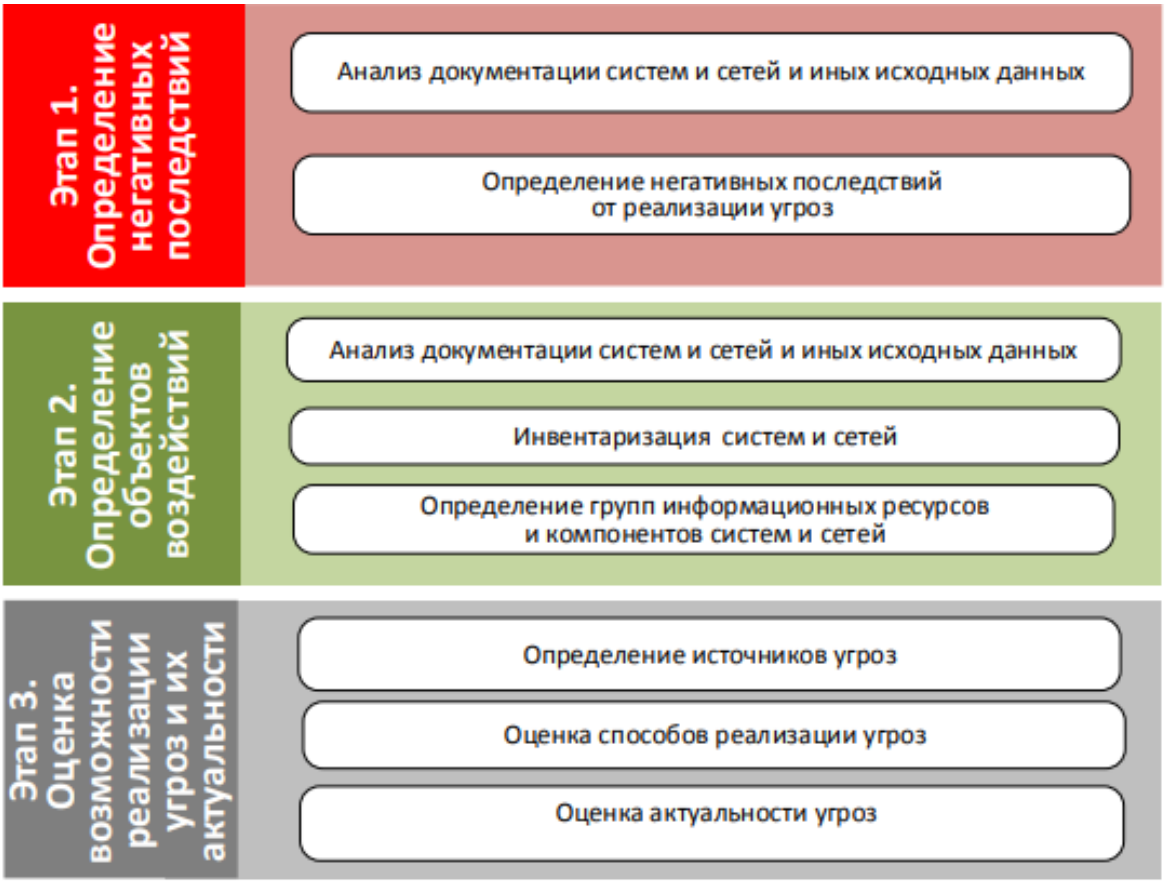
Цель: получить опыт определения угроз информационной безопасности на основе актуальной методики.

Теоретические сведения

Оценка угроз безопасности информации проводится в целях определения угроз безопасности информации, реализация (возникновение) которых возможна в системах и сетях с заданной архитектурой и в условиях их функционирования – актуальных угроз безопасности информации.

Основными задачами, решаемыми в ходе оценки угроз безопасности информации, являются:

а) определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации;
б) инвентаризация систем и сетей и определение возможных объектов воздействия угроз безопасности информации;
в) определение источников угроз безопасности информации и оценка возможностей нарушителей по реализации угроз безопасности информации;
г) оценка способов реализации (возникновения) угроз безопасности информации;
д) оценка возможности реализации (возникновения) угроз безопасности информации и определение актуальности угроз безопасности информации;
е) оценка сценариев реализации угроз безопасности информации в системах и сетях



Общая схема проведения оценки угроз безопасности информации

Вебинар от Инфосистемы Джет (есть примеры) - https://youtu.be/rzDAJS0QVww

Сайт Банк данных угроз информации – bdu.fstec.ru

Практическое задание

На основе методики заполнить рекомендуемую структуру модели угроз безопасности информации (Приложение 3) для организации согласно варианту. Для заполнения документа необходимо пользоваться приложениями методики, в которых есть множество пояснений и примеров.

Структура модели угроз:

1. Общие положения – Заполните согласно приложения 3, постарайтесь максимально хорошо проанализировать деятельность организации.
2. Описание систем и сетей и их характеристика как объектов защиты - Заполните согласно приложения 3, постарайтесь максимально хорошо проанализировать деятельность организации
3. Возможные негативные последствия от реализации (возникновения) угроз безопасности информации
4. Возможные объекты воздействия угроз безопасности информации
5. Источники угроз безопасности информации
6. Способы реализации (возникновения) угроз безопасности информации
7. Актуальные угрозы безопасности информации

Варианты для выполнения задания:

1. Школа
2. Поликлиника
3. Рекламное агентство
4. Научно-исследовательский институт
5. Районный суд
6. Университет
7. ТЭЦ
8. Районный суд
9. Автосалон
10. Фармацевтическая компания
11. Автошкола
12. Патентное бюро
13. Районный отдел полиции
14. МФЦ
15. Добывающая компания (золото)
16. Банк
17. Музей
18. Редакция научного издания

Приложение 1 – Скриншоты примера построения модели угроз

ИСХОДНЫЕ ДАННЫЕ ПО ИС ДЛЯ ПРИМЕРА

1. **Коммерческая страховая организация**
2. **Назначение системы:** урегулирование убытков
3. **Тип обрабатываемой информации:** персональные данные клиентов
4. **Категория ИС:** незначимый объект КИИ, ИСПДн
5. **Используемые средства защиты:**
   - СКЗИ для подключения к инфраструктуре в ЦОД
   - Межсетевой экран на периметрах ЛВС
   - Антивирусные средства защиты на АРМ пользователей и серверах под управлением ОС Windows
   - Используется сканер защищенности, но не для всех компонентов ИТ-инфраструктуры
   - Внедрены меры защиты в соответствии с концепцией Security Development Lifecycle

ОПРЕДЕЛЕНИЕ НЕГАТИВНЫХ ПОСЛЕДСТВИЙ
ЭТАП 1

У1

1. Финансовый, иной материальный ущерб физическому лицу
2. Утечка персональных данных
3. Разглашение персональных данных граждан

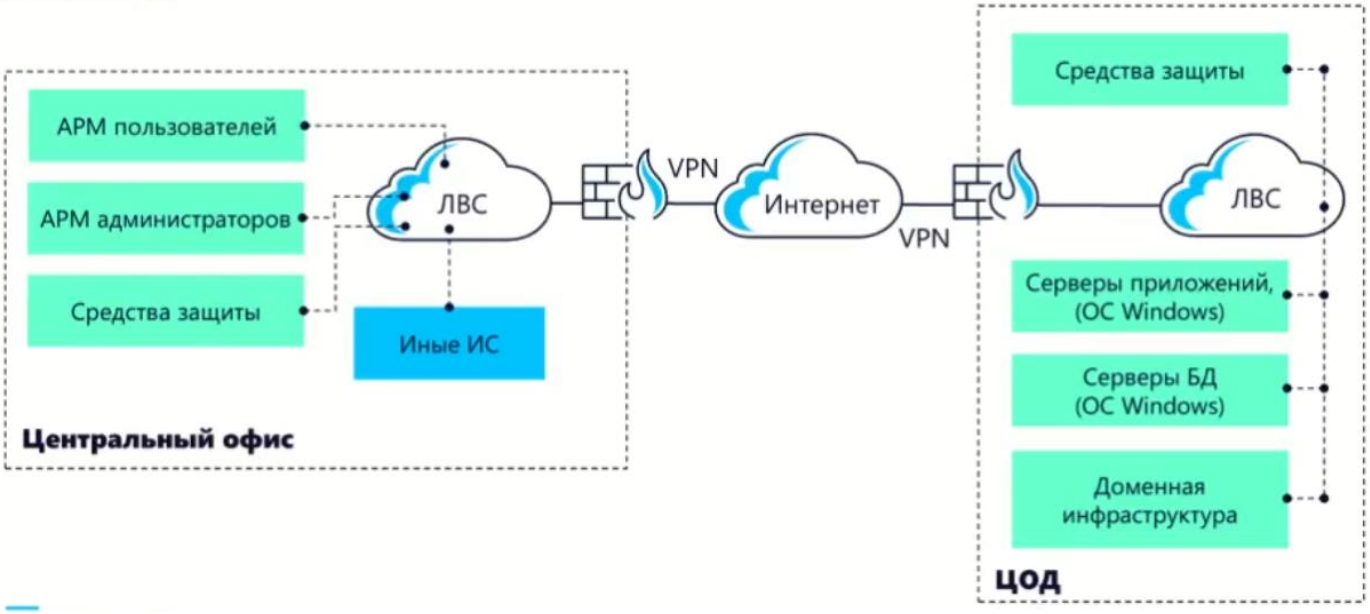
У2

1. Нарушение законодательства РФ
2. Необходимость затрат на закупку технических средств, вышедших из строя
3. Простой информационной системы или сети
4. Утрата доверия

У3

Возникновение ущерба бюджетам Российской Федерации

ОПРЕДЕЛЕНИЕ ОБЪЕКТОВ ВОЗДЕЙСТВИЯ (1/3)
ЭТАП 2



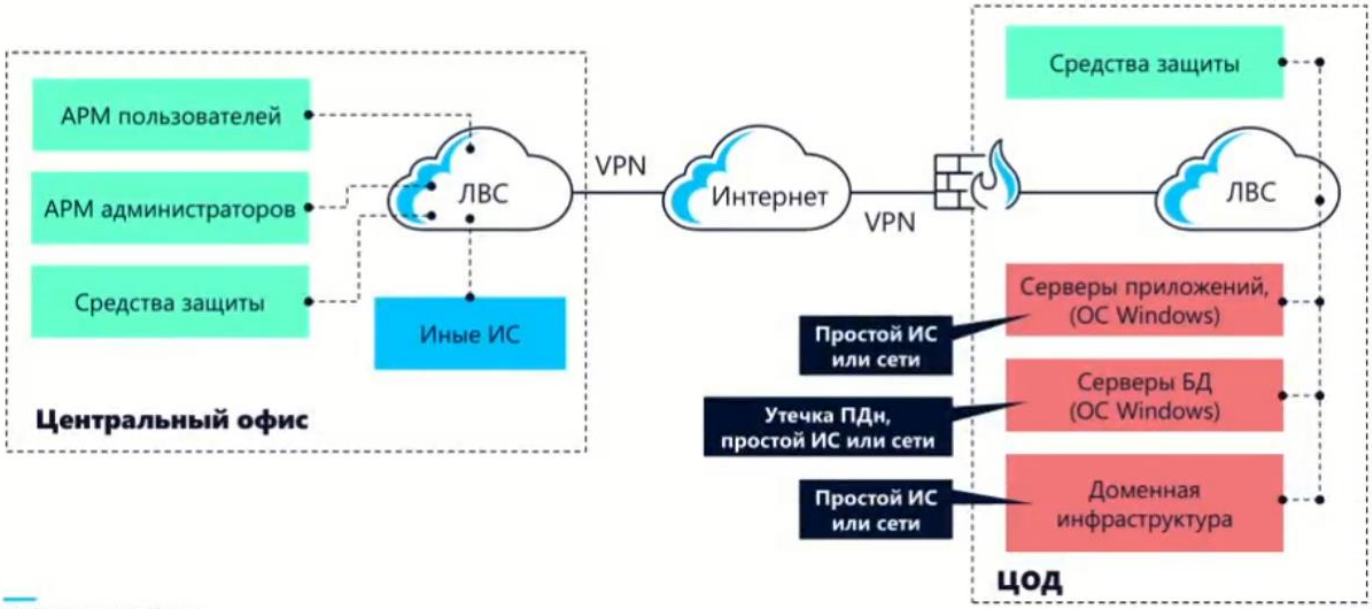
ОПРЕДЕЛЕНИЕ ВИДОВ ВОЗДЕЙСТВИЯ НА ОБЪЕКТЫ (2/3) ЭТАП 2

Негативные последствия	Объекты воздействия	Виды воздействия
Утечка персональных данных	Серверы БД	• Модификация данных • Несанкционированный доступ
Простой информационной системы или сети	• Серверы инфраструктуры • Серверы БД • Серверы приложений	Отказ в обслуживании

МОДЕЛИРОВАНИЕ ВОЗМОЖНЫХ НАРУШИТЕЛЕЙ (1/2) ЭТАП 3

Тип нарушителя	У1	У2	У3	Оценка актуальности
Специальные службы иностранных государств	–	–	–	Неактуальный
Преступные группы (криминальные структуры)	+	+	–	Актуальный
Отдельные физические лица (хакеры)	+	+	–	Актуальный
Конкурирующие компании	–	+	–	Актуальный

СОПОСТАВЛЕНИЕ ОБЪЕКТОВ ВОЗДЕЙСТВИЯ И НЕГАТИВНЫХ ПОСЛЕДСТВИЙ (3/3) ЭТАП 2



МОДЕЛИРОВАНИЕ ВОЗМОЖНЫХ НАРУШИТЕЛЕЙ (2/2) ЭТАП 3

Тип нарушителя	У1	У2	У3	Оценка актуальности
Разработчики программных, программно-аппаратных средств	+	+	–	Актуальный
Авторизованные пользователи систем и сетей	+	+	–	Актуальный
Системные администраторы и администраторы безопасности	+	+	–	Актуальный
Бывшие работники (пользователи)	–	+	–	Актуальный

СПОСОБЫ РЕАЛИЗАЦИИ УГРОЗ ЭТАП 3

Актуальный тип нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации
Отдельные физические лица (хакеры)	Серверы БД: утечка ПДн	Внешние сетевые интерфейсы	• Использование уязвимостей • Внедрение ВПО
		Внутренние сетевые интерфейсы	• Использование уязвимостей • Внедрение ВПО
		Интерфейсы для использования съемных носителей	Внедрение ВПО

СЦЕНАРИИ ЭТАП 3

В рамках текущего вебинара рассмотрим негативное последствие:

Утечка ПДн

Для выбранного негативного последствия рассмотрим для примера три выбранных сценария:

- Компрометация учетных записей пользователей рассматриваемой ИС
- Распространение ВПО через съемный носитель информации
- Нарушение правил административного доступа

КОМПРОМЕТАЦИЯ УЧЕТНЫХ ЗАПИСЕЙ ПОЛЬЗОВАТЕЛЕЙ РАССМАТРИВАЕМОЙ ИС (1/2) ЭТАП 3

ТАКТИКА	ТЕХНИКИ	ВОЗМОЖНОСТЬ РЕАЛИЗАЦИИ ТЕХНИКИ И ОБОСНОВАНИЙ В СЛУЧАЕ НЕВОЗМОЖНОСТИ	УГРОЗЫ ИЗ БДУ ФСТЭК	АКТУАЛЬНОСТЬ УГРОЗЫ
Т1 (Сбор информации о системах и сетях)	Т1.12 (Сбор личной идентификационной информации)	Реализация возможна	-	-
	Т1.15 (Поиск и покупка баз данных, скомпрометированных паролей и ключей)	Реализация возможна	-	-
Т2 (Получение первоначального доступа)	Т2.1 (Использование внешних сервисов в сети Интернет)	Внешний сервис рассматриваемого объекта в ЦОД доступен по VPN. В центральном офисе отсутствуют внешние сервисы в сеть Интернет. Выполняется проверка паролей по умолчанию автоматизированным способом по словарям Также проводятся внутренние проверки	-	-

КОМПРОМЕТАЦИЯ УЧЕТНЫХ ЗАПИСЕЙ ПОЛЬЗОВАТЕЛЕЙ РАССМАТРИВАЕМОЙ ИС (2/2) ЭТАП 3

ТАКТИКА	ТЕХНИКИ	ВОЗМОЖНОСТЬ РЕАЛИЗАЦИИ ТЕХНИКИ И ОБОСНОВАНИЙ В СЛУЧАЕ НЕВОЗМОЖНОСТИ	УГРОЗЫ ИЗ БДУ ФСТЭК	АКТУАЛЬНОСТЬ УГРОЗЫ
Т2 (Получение первоначальног о доступа)	Т2.4 (Использование слабых паролей и паролей по умолчанию)	Выполняется проверка паролей по умолчанию автоматизированным способом по словарям Также проводятся внутренние проверки и настроена сложность парольной политики в соответствии с внутренними документами	УБИ.030	Неактуальная
	Т2.10 (Подбор паролей)	Установлено время блокировки учетной записи в случае неправильного ввода пароля. Настроена сложность парольной политики в соответствии с внутренними документами	УБИ.008	Неактуальная
	Т2.11 (НСД путем компрометации личных данных данных)	Реализация возможна	УБИ.074	Актуальная
	Т2.14 (Обход биометрической аутентификации)	Не применима	-	-

РАСПРОСТРАНЕНИЕ ВПО ЧЕРЕЗ СЪЕМНЫЙ НОСИТЕЛЬ ИНФОРМАЦИИ (1/2) ЭТАП 3

ТАКТИКА	ТЕХНИКИ	ВОЗМОЖНОСТЬ РЕАЛИЗАЦИИ ТЕХНИКИ И ОБОСНОВАНИЙ В СЛУЧАЕ НЕВОЗМОЖНОСТИ	УГРОЗЫ ИЗ БДУ ФСТЭК	АКТУАЛЬНОСТЬ УГРОЗЫ
Т1 (Сбор информации о системах и сетях)	Т1.1 (Сбор информации в сети Интернет)	Реализация возможна	-	-
	Т1.11 (Сбор информации путем использования техник социальной инженерии)	Реализация возможна	-	-
Т2 (Получение первоначальног о доступа)	Т2.7 (Использование внешних носителей с вредоносным ПО)	Проводятся мероприятия по повышению осведомлённости ИБ, возможность подключения съемных носителей ограничена. Комплекс используемых средств защиты	УБИ.006	Неактуальная

РАСПРОСТРАНЕНИЕ ВПО ЧЕРЕЗ СЪЕМНЫЙ НОСИТЕЛЬ ИНФОРМАЦИИ (2/2) ЭТАП 3

ТАКТИКА	ТЕХНИКИ	ВОЗМОЖНОСТЬ РЕАЛИЗАЦИИ ТЕХНИКИ И ОБОСНОВАНИЙ В СЛУЧАЕ НЕВОЗМОЖНОСТИ	УГРОЗЫ ИЗ БДУ ФСТЭК	АКТУАЛЬНОСТЬ УГРОЗЫ
Т3 (Внедрение и исполнение вредоносного кода)	Т3.1 (автоматический запуск скриптов и исполняемых файлов с использованием методов социальной инженерии)	Не рассматривается в виду невозможности реализации предшествующих техник, но возможно в рамках других сценариях	УБИ.006	-
	Т3.15 (Планирование запуска вредоносных программ через планировщик задач)	Не рассматривается в виду невозможности реализации предшествующих техник, но возможно в рамках других сценариях	УБИ.006	-
Т4 (Закрепление в системе)	Т4.5 (Внесение соответствующих записей в реестр, автозагрузку, планировщики заданий, обеспечивающих запуск вредоносного ПО при перезагрузке)	Не рассматривается в виду невозможности реализации предшествующих техник, но возможно в рамках других сценариях	УБИ.121	-
Т5 (Управление вредоносным ПО)	Т5.6 (Проксирование трафика управления для маскировки подозрительной сетевой активности)	Не рассматривается в виду невозможности реализации предшествующих техник, но возможно в рамках других сценариях	-	-

НАРУШЕНИЕ ПРАВИЛ АДМИНИСТРАТИВНОГО ДОСТУПА ЭТАП 3

ТАКТИКА	ТЕХНИКИ	ВОЗМОЖНОСТЬ РЕАЛИЗАЦИИ ТЕХНИКИ И ОБОСНОВАНИЙ В СЛУЧАЕ НЕВОЗМОЖНОСТИ	УГРОЗЫ ИЗ БДУ ФСТЭК	АКТУАЛЬНОСТЬ УГРОЗЫ
Т6 (Повышение привилегий по доступу к компонентам)	Т6.3 (Эксплуатация уязвимостей ПО к повышению привилегий)	Реализация возможна	УБИ.122	Актуальная
Т9 (Сбор и вывод из системы для дальнейших действий при реализации угроз)	Т9.7 (Проксирование трафика управления для маскировки подозрительной сетевой активности)	Реализация возможна	-	-
Т10 (Несанкционированный доступ)	Т10.1 (НСД к защищаемой информации)	Реализация возможна	УБИ.078, УБИ.088	Актуальная