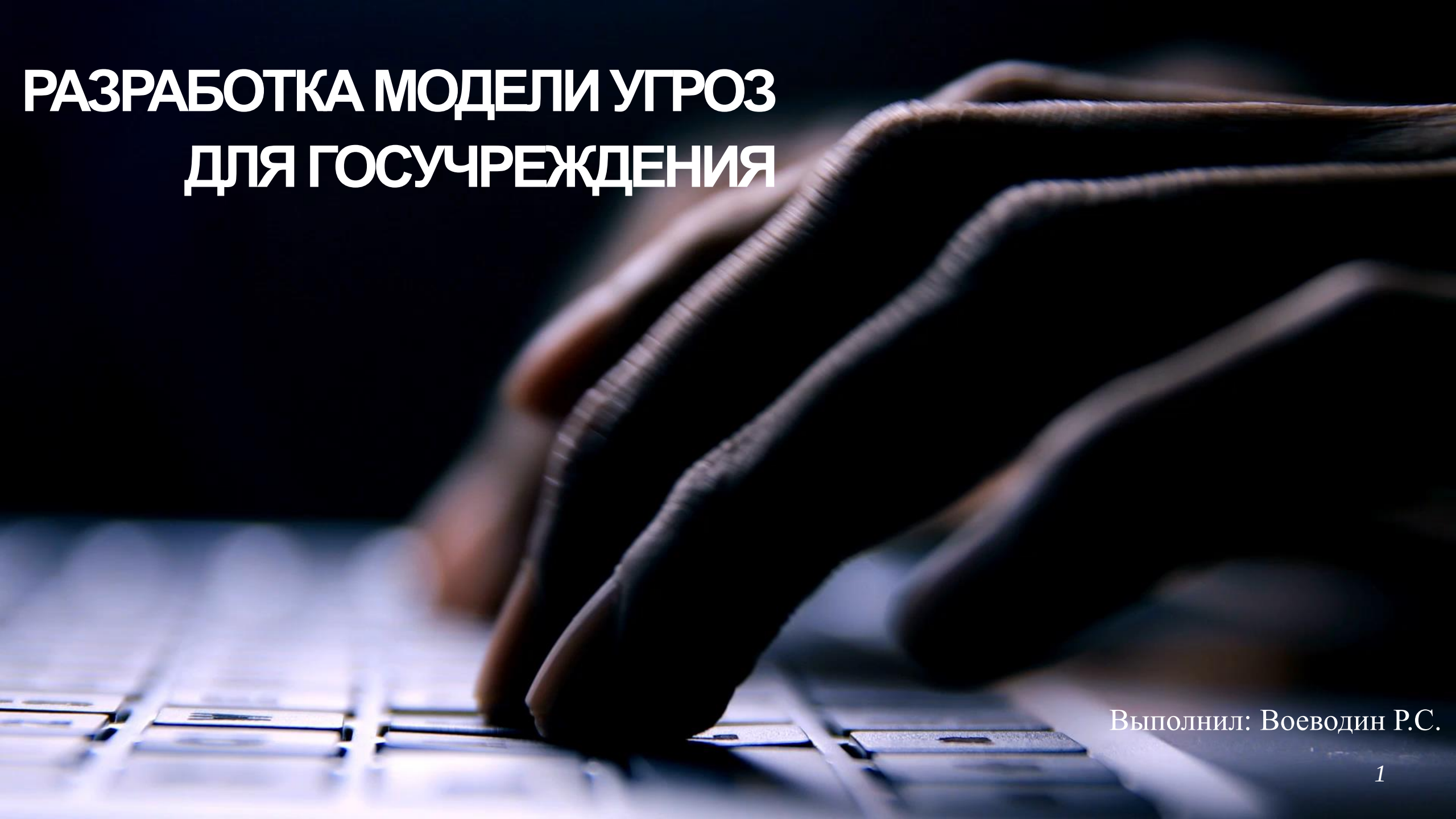


РАЗРАБОТКА МОДЕЛИ УГРОЗ ДЛЯ ГОСУЧРЕЖДЕНИЯ

Выполнил: Воеводин Р.С.

Данная модель была разработана для государственного архива Санкт-Петербурга, для согласования КИС. При Соблюдение норм и стандартов, удовлетворяющих требования ФСТЭК и КИС.

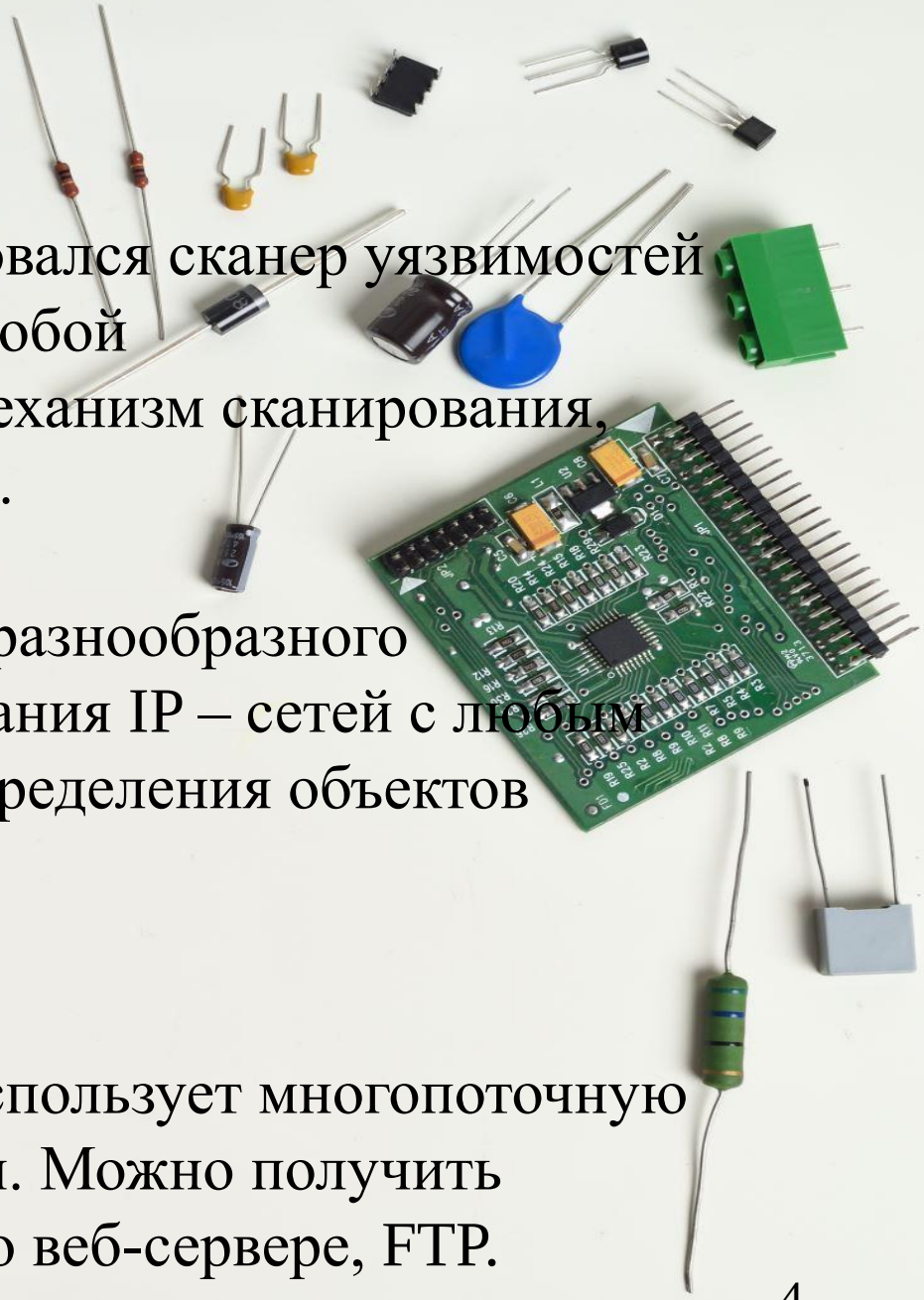
ЦЕЛЬ РАБОТЫ

- Разработать модель угроз
- Провести аудит информационной системы

Задачи:

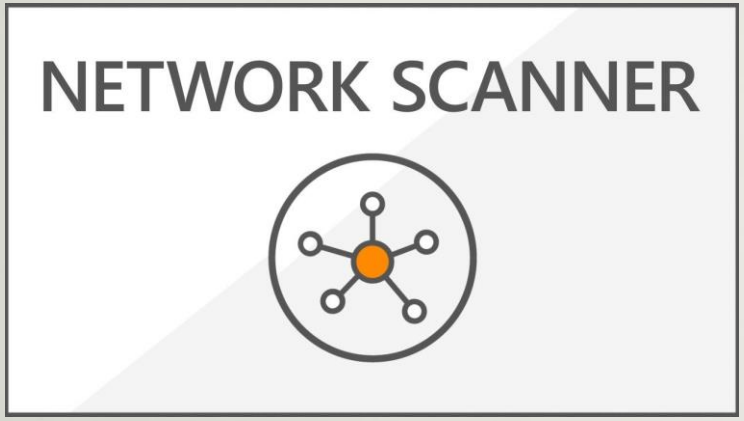
1. Внутрисегментное сканирование(использование сканеров уязвимостей)
2. Исследование на наличие уязвимостей
3. Поиск слабых мест в системе
4. Разработка модели угроз

ВЫБОР ПО

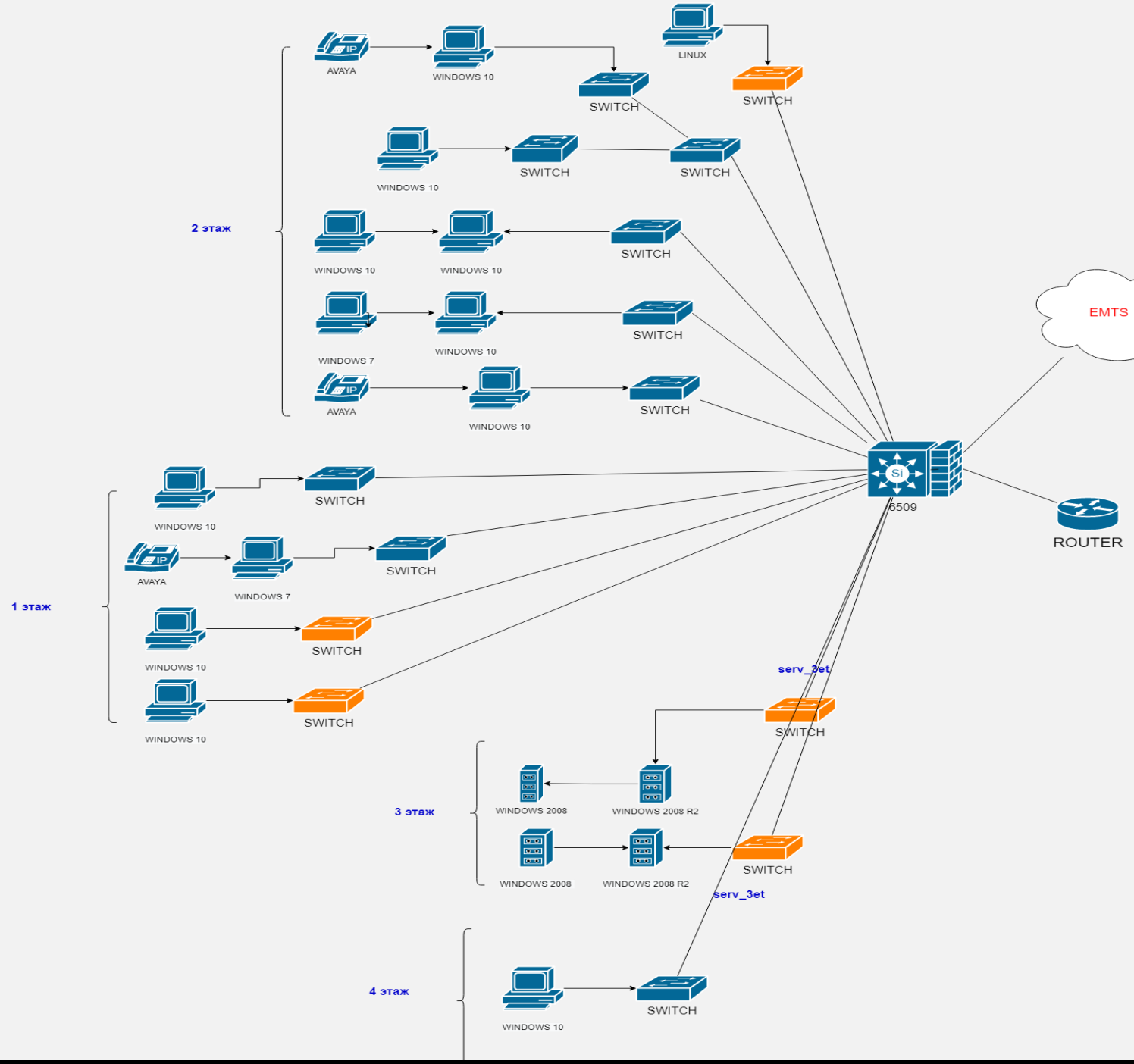


В данной работе использовался сканер уязвимостей OpenVAS. Представляет собой полнофункциональный механизм сканирования, работает без ограничений.

NMAP предназначен для разнообразного настраиваемого сканирования IP – сетей с любым количеством объектов, определения объектов сканируемой сети.



NETWORK SCANNER использует многопоточную технологию сканирования. Можно получить информацию о NetBIOS, о веб-сервере, FTP.



Состав сети

Рабочие станции – 650+

Рабочие станции на Windows 10 – 590 ПК

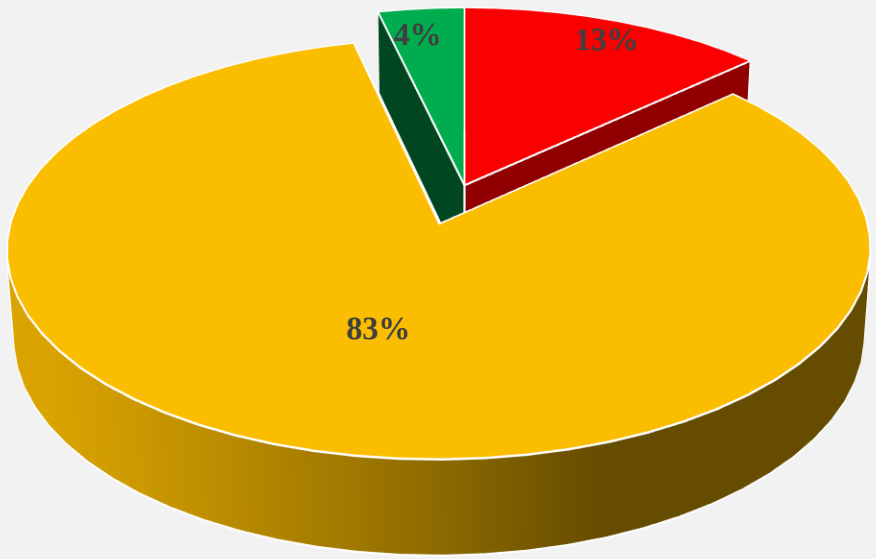
Рабочие станции на Windows 7 – 55 ПК

Рабочие станции на Linux – 5 ПК

*КРИТИЧЕСКИЙ ВАЖНЫЕ СЕРВИСЫ И ПРОТОКОЛЫ, ОБНАРУЖЕННЫЕ ПРИ СКАНИРОВАНИИ

Порт	21	22	80	135	443	445	3389
Описание	Использует протокол управления передачей данных (TCP), который является одним из основных протоколов в сетях TCP/IP SCTP/TCP/UDP	TCP является протоколом с установлением соединения и требует квитирования для установки сквозной связи. SCTP/TCP/UDP	Используется для незашифрованного трафика HTTP SCTP/TCP/UDP	Используется службами удаленного обслуживания (DHCP, DNS,WINS) TCP/UDP	Используется для передачи данных по HTTPS SCTP/TCP/UDP	Используется для совместной работы с файлами TCP	Стандартный порт подключения по RDP-уязвимость, которая позволяет атакующему не прошедшему проверку подлинности, через RDP выполнить код на целевой системе TCP/UDP*
Сервисы	FTP	SSH	HTTP	Epmap, MSRPC, LOC-SRV	HTTPS	Microsoft-DS AD, SMB	RDP

Задача № 2. Исследование уязвимостей



Количество уязвимостей в разных сетях	1 сеть	2 сеть	3 сеть
Высокий уровень опасности	10	5	10
Средний уровень опасности	132	22	4
Малый уровень опасности	4	2	1

Общее количество уязвимых мест - **190**.

КАК СТРОИТСЯ МОДЕЛЬ УГРОЗ?

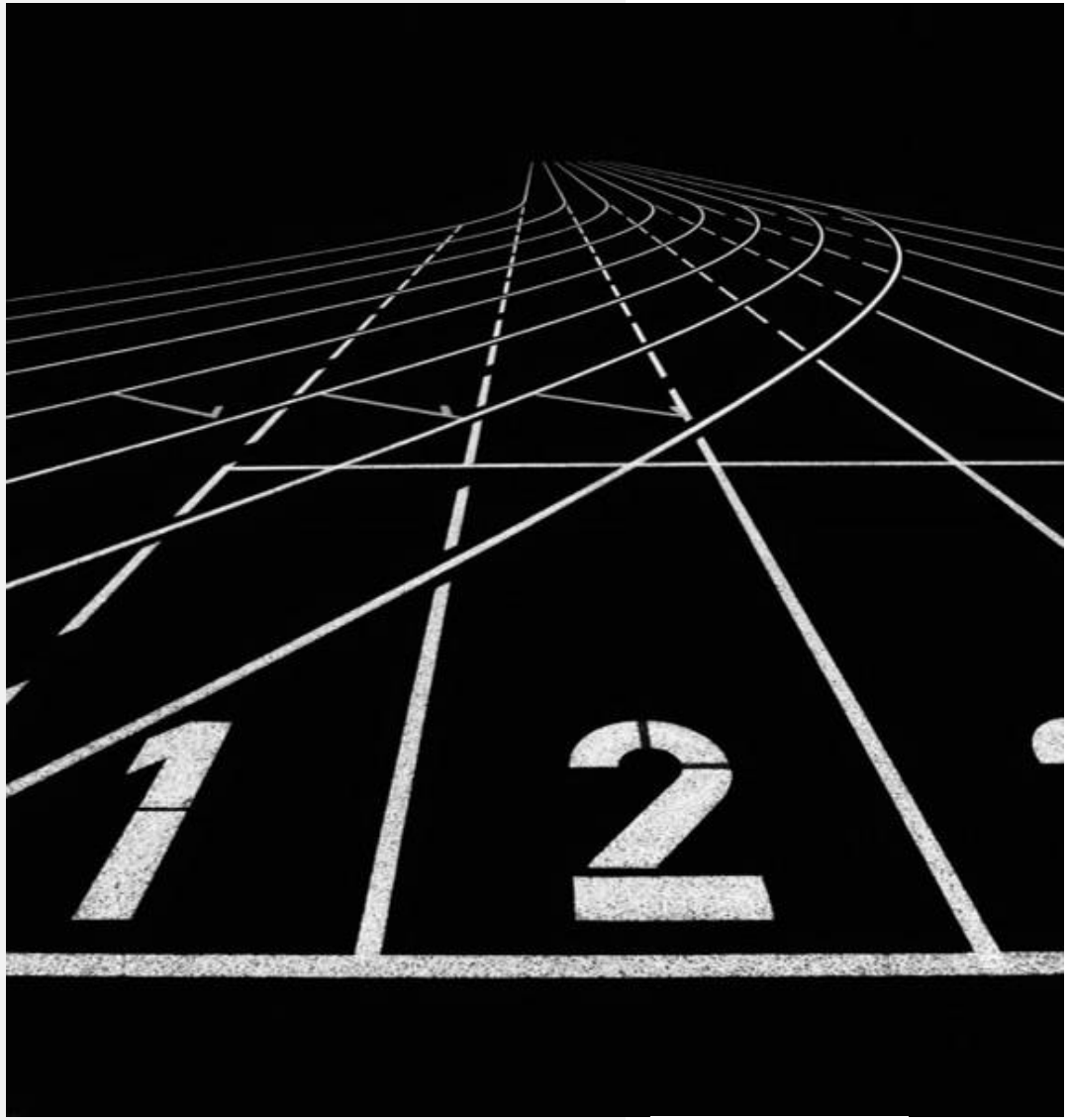
В данной работе мы используем методику: «Меры защиты информации в государственных системах»

Этап оценки угрозы:

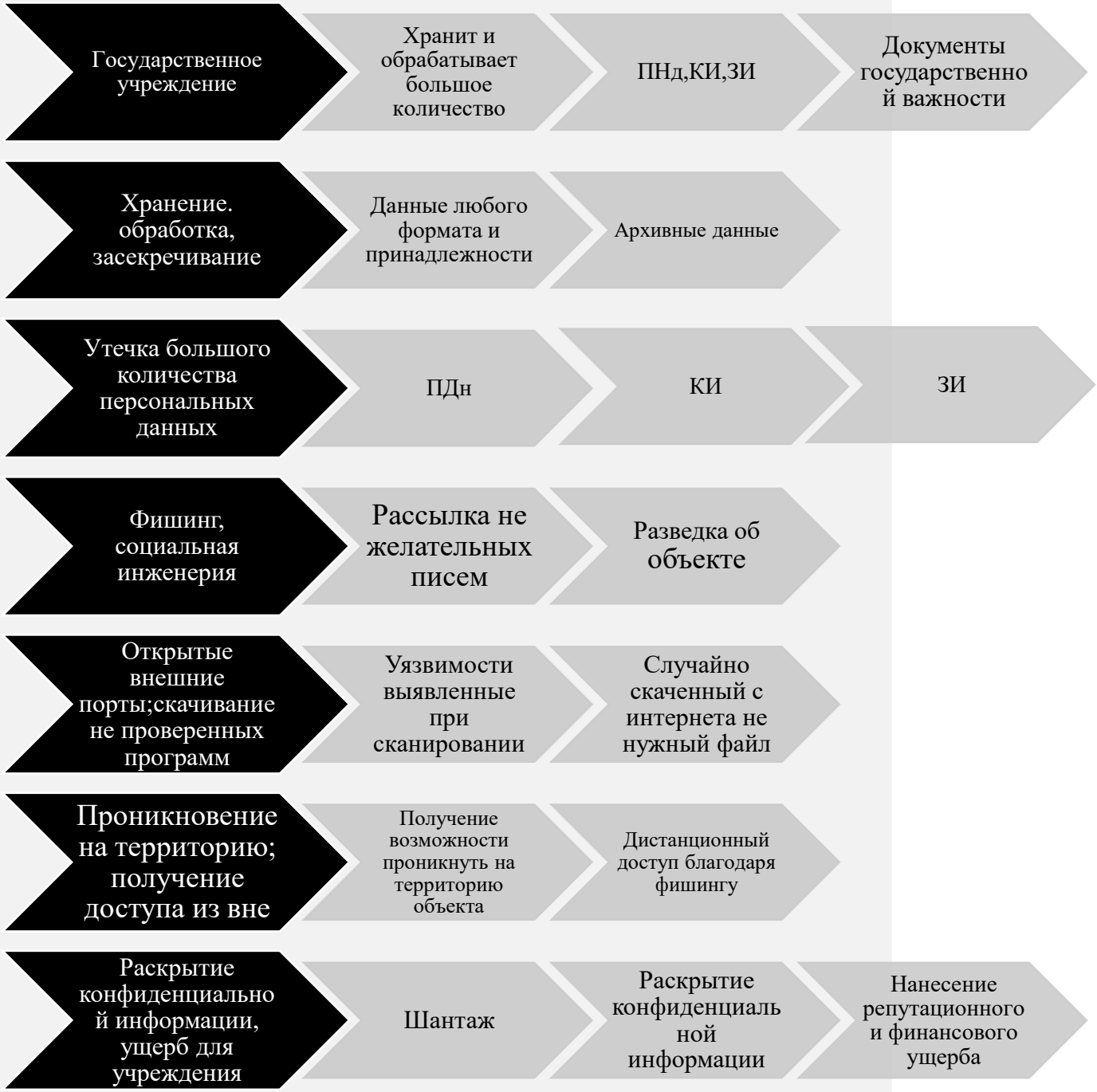
1. Определение негативных последствий
2. Объекты воздействия
3. Модель нарушителя
4. Способы реализации угрозы
5. Возможные сценарии

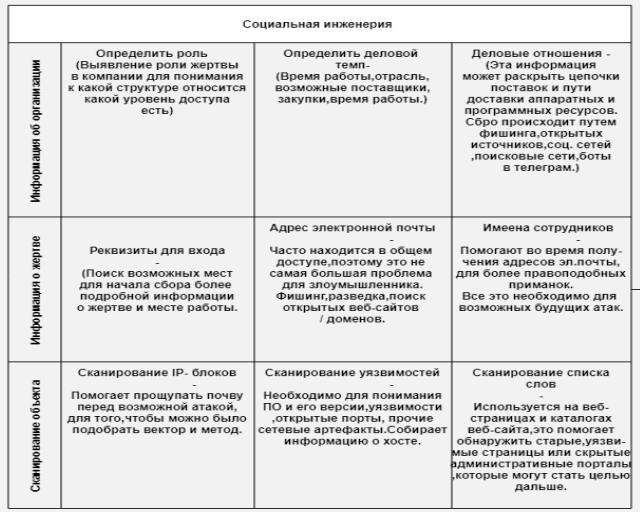
Берем все угрозы и исключаем те, которые:

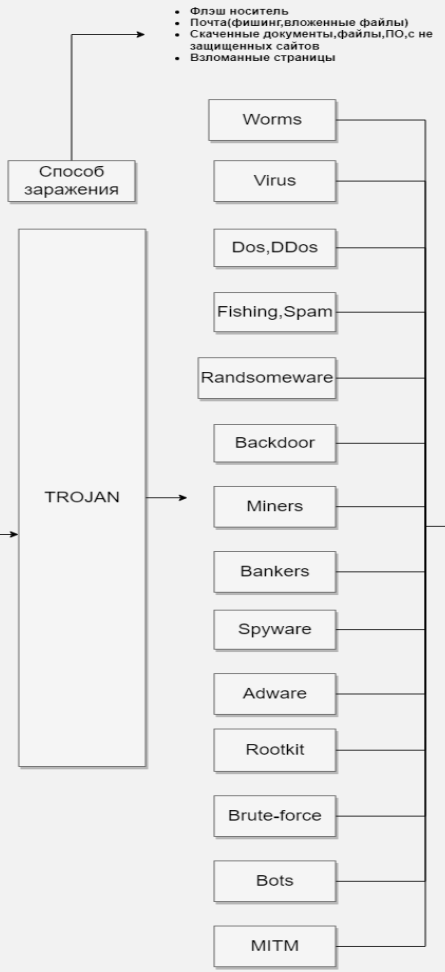
1. Не приводят к негативным последствиям(ущербу)
2. Не связаны с нарушителями нужного типа с нужными ему целями
3. Требуют от нарушителей доступа, которого у них нет

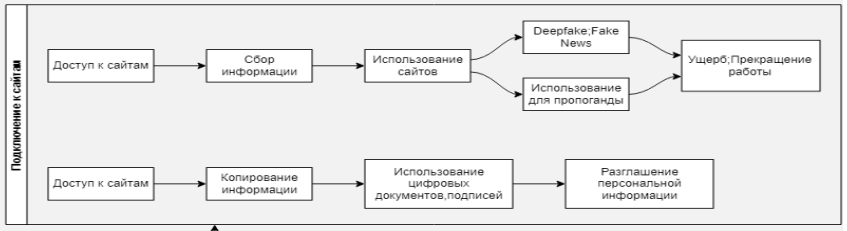


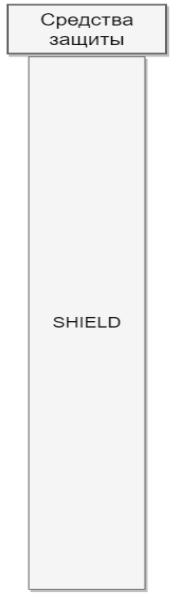
ПОЭТАПНОЕ ПОСТРОЕНИЕ МОДЕЛИ УГРОЗ

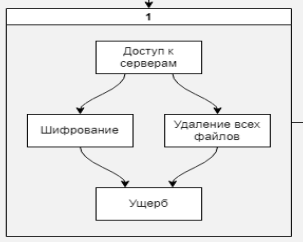












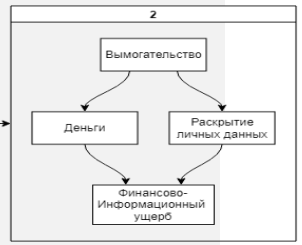


ДИАГРАММА ВОЗМОЖНЫХ РАЗВИТИЙ СОБЫТИЙ ВНУТРИ СЕТИ

WAF

Web Application Firewall,совокупность мониторов и фильтров,предназначенных для обнаружения и блокирования сетевых атак на веб-приложения.

DLP

Data Loss Prevention-технология предотвращения утечек конфиденциальной информации из информационной системы.

SIEM

Security information and event managment - управление событиями и информацией о безопасности.

МЕРЫ ЗАЩИТЫ ПО ПРЕДОТВРАЩЕНИЮ ИНЦИДЕНТОВ ВНУТРИ ОРГАНИЗАЦИИ

- Антивирусная защита
- Аудит безопасности
- Защита информационной системы и её компонентов
- Идентификация и аутентификация
- Реагирование на компьютерные инциденты
- Информирование и обучение персонала
- Обеспечение доступности
- Управление обновлениями ПО
- Ограничение программной среды
- Предотвращение вторжений
- Управление конфигурацией
- Управление доступом

Заключение

1. *Все поставленные задачи были выполнены.*
2. *Проведенный аудит был изучен специалистами информационной безопасности нашего комитета.*
3. *Меры по закрытию возможных уязвимостей были отправлены в работу.*
4. *Были проведены необходимые испытания.*
5. *Модель была разработана, одобрена и апробирована и отправлена на согласование в КИС.*