

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ
ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Поволжский государственный университет телекоммуникаций и информатики»

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

РАЗРАБОТКА ЗАЩИТЫ ДАННЫХ КОРПОРАТИВНОЙ СЕТИ ОРГАНИЗАЦИИ

ВЫПОЛНИЛ: СТУДЕНТ ГРУППЫ ИБТС-81

РОГОЖИН А.В.

РУКОВОДИТЕЛЬ: К.Т.Н., ДОЦЕНТ КАФЕДРЫ ИБ

БЕЛЬСКАЯ Н.М.

Цель ВКР:

Разработка системы обеспечения безопасности данных корпоративной сети организации.

Задачи:

- Рассмотреть особенности защиты данных в компьютерных сетях
- Изучить методы и средства защиты данных в сети
- Организовать защиту данных в сети организации
- Произвести расчёт рисков ИБ

Виды информационных ресурсов



Классификация информационных ресурсов

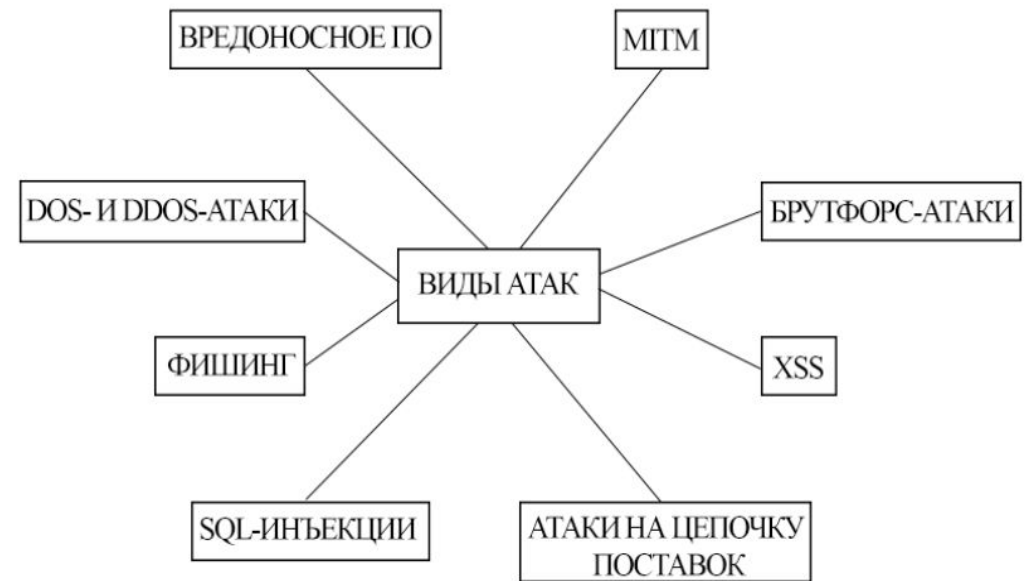


Классификация информации по категориям доступа

Основные виды атак на данные в КС и способы защиты от них

Рекомендованные меры безопасности:

- Шифрование данных
- Сильные и уникальные пароли
- Своевременное Обновление ПО
- Обучение пользователей
- Мониторинг и обнаружение
- Регулярные аудиты безопасности



Основные виды атак на данные

Особенности работы удаленных пользователей

Преимущества:

- Защита от физических угроз
- Облачные технологии
- Безопасная передача данных

Недостатки:

- Уязвимость домашнего Wi-Fi
- Нарушение политики доступа
- Отсутствие антивирусных программ

Три основные технологии реализации удаленного доступа:

- Веб-сервисы
- Remote Desktop Services (RDS) и VPN
- VDI (виртуализация рабочего стола)

Средства и методы защиты данных в сети

Антивирусное программное обеспечение – это специальные программы, созданные для обнаружения, блокировки и удаления вредоносных программ, таких как вирусы, трояны, шпионское ПО и другие формы вредоносного кода.

Системы обнаружения вторжений предоставляют моментальное реагирование на потенциальные атаки, но и обеспечивают анализ сетевой активности для выявления необычных паттернов и поведения.

Межсетевой экран представляет собой программно-аппаратный или программный комплекс, который активно отслеживает передвижение сетевых пакетов, решая, блокировать их или разрешить прохождение.

Виртуальная частная сеть (VPN) представляет собой технологию, обеспечивающую безопасное и зашифрованное соединение между удаленными узлами через открытую сеть, такую как интернет.

Схема сети организации и используемое оборудование

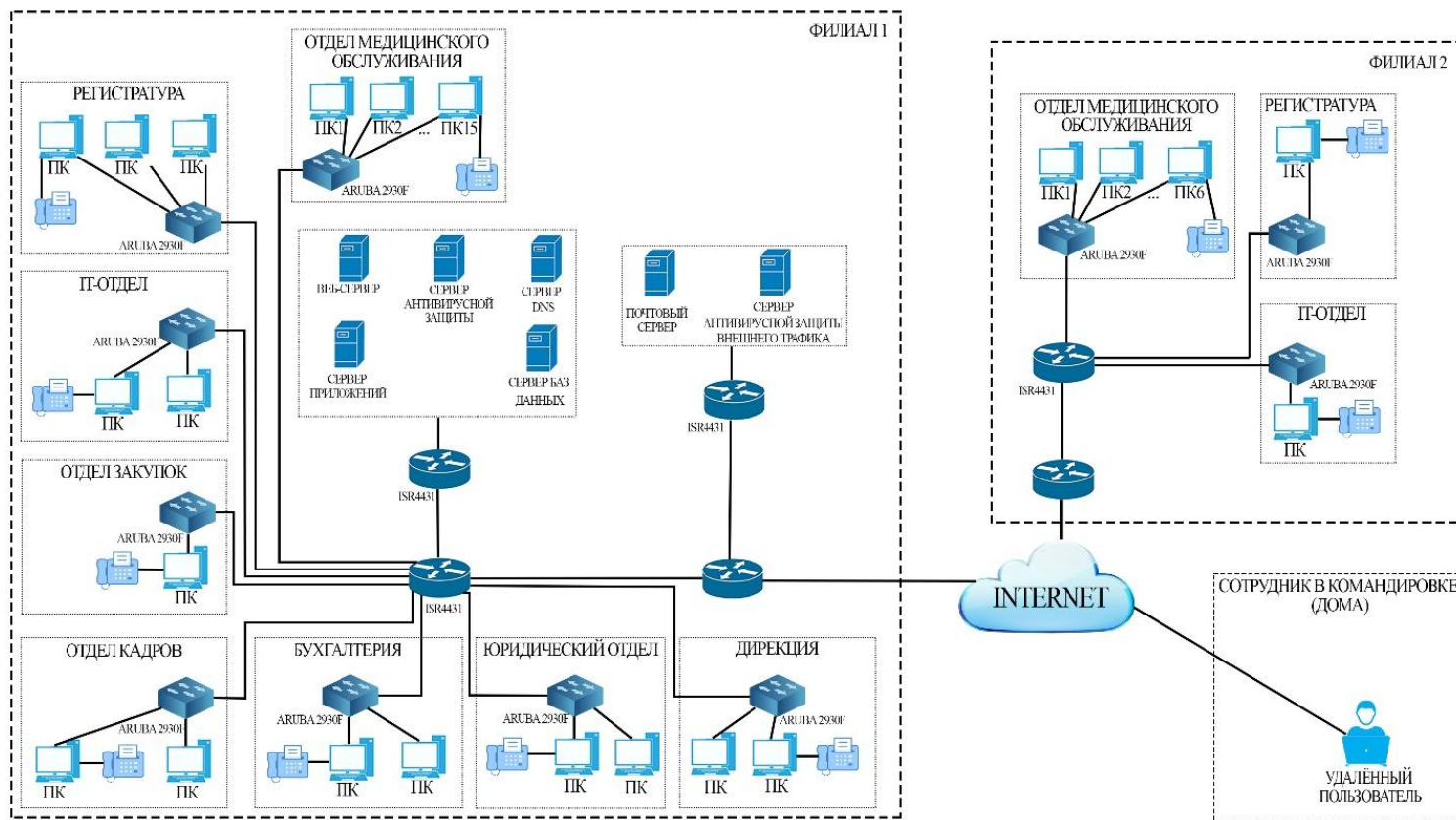


Схема сети организации



Коммутатор HPE Aruba 2930F



Маршрутизатор Cisco ISR4431

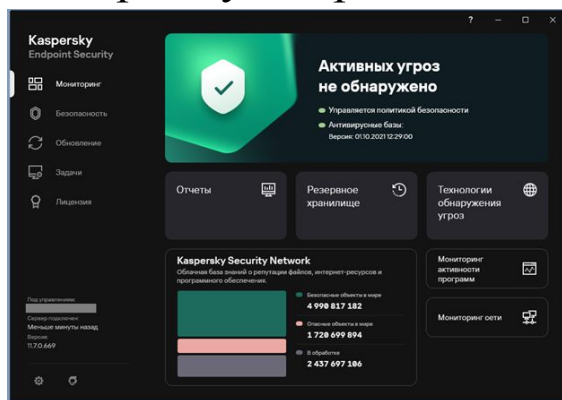
Схема сети со средствами защиты

Предложенные средства защиты:

- МЭ ZYXEL ZyWALL ATR200



- Kaspersky Endpoint Security



- OpenVPN

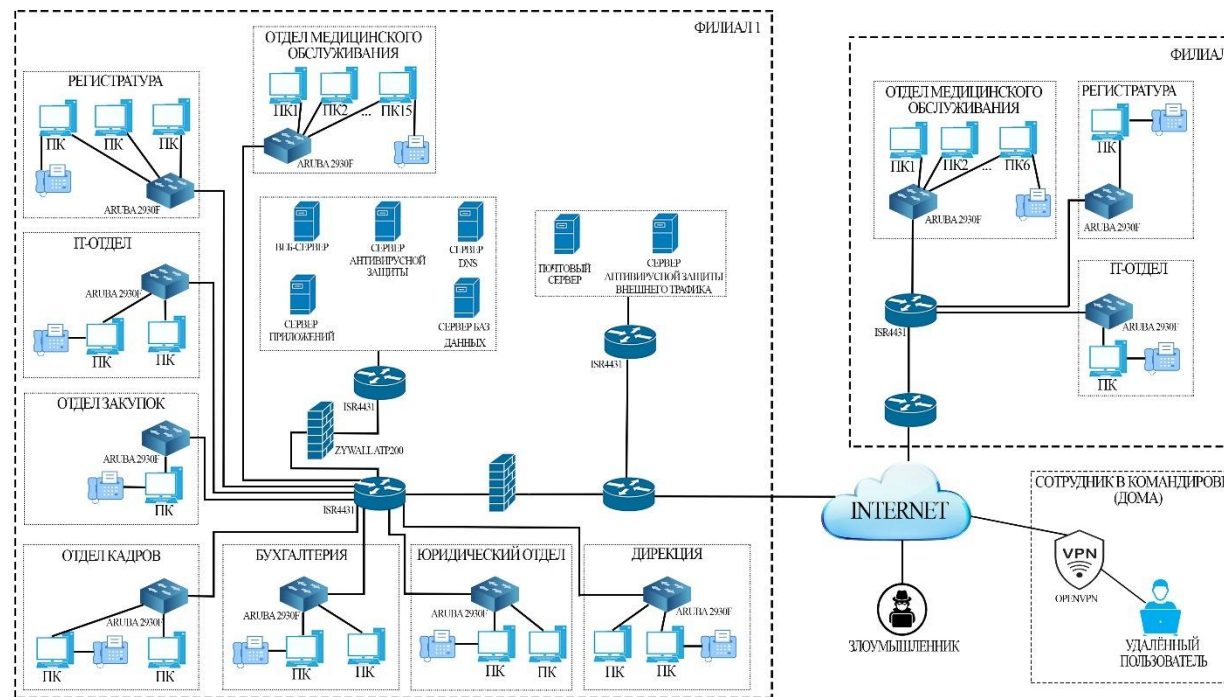
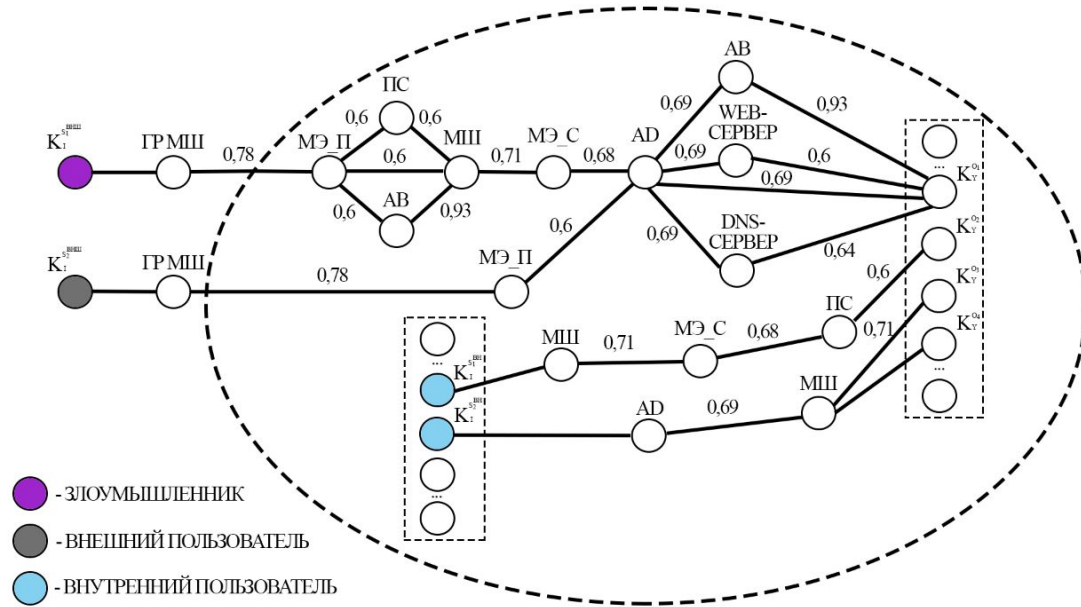


Схема сети со средствами защиты

Расчёт рисков ИБ



Нечёткая когнитивная карта

Вероятность реализации угрозы по выбранному пути:

$$P_l = P_{\text{АКТ}} \cdot \prod_{z \in Z} w_{z,z+1}$$

где $P_{\text{АКТ}}$ - вероятность активизации входного концепта, $w_{z,z+1}$ - значение уязвимости компонента инфраструктуры, представленного в НКК промежуточным компонентом K'_{z+1}

Величина относительного риска:

$$\overline{R_{O_h}} = P^U(K_i \rightarrow K_y) \cdot \frac{c^{O_h}}{c_{\Sigma}}$$

где $\frac{c^{O_h}}{c_{\Sigma}}$ - относительная стоимость информационного ресурса

Величина полного относительного риска:

$$\overline{R_1} = \sum_{h=1}^H \overline{R_{O_h}}$$

где $\overline{R_{O_h}}$ - величина относительного риска

Результаты расчетов

	Тип угрозы	P_i	$\overline{R_{O_1}}$	$\overline{R_{O_2}}$	$\overline{R_{O_3}}$	$\overline{R_{O_4}}$	\overline{R}
Расчет 1	Злоумышленник	0.0312	0.0249	-	-	-	0.1430
	Внешний пользователь	0.0989	0.0791	-	-	-	
	Внутренний пользователь (для пути 1)	0.1448	-	0.0145	-	-	
	Внутренний пользователь (для пути 2)	0.2449	-	-	0.0147	0.0098	
Расчет 2	Злоумышленник	0.0359	0.0287	-	-	-	0.1374
	Внешний пользователь	0.0872	0.0697	-	-	-	
	Внутренний пользователь (для пути 1)	0.1448	-	0.0145	-	-	
	Внутренний пользователь (для пути 2)	0.2449	-	-	0.0147	0.0098	
Расчет 3	Злоумышленник	0.0405	0.0324	-	-	-	0.1348
	Внешний пользователь	0.0792	0.0634	-	-	-	
	Внутренний пользователь (для пути 1)	0.1448	-	0.0145	-	-	
	Внутренний пользователь (для пути 2)	0.2449	-	-	0.0147	0.0098	

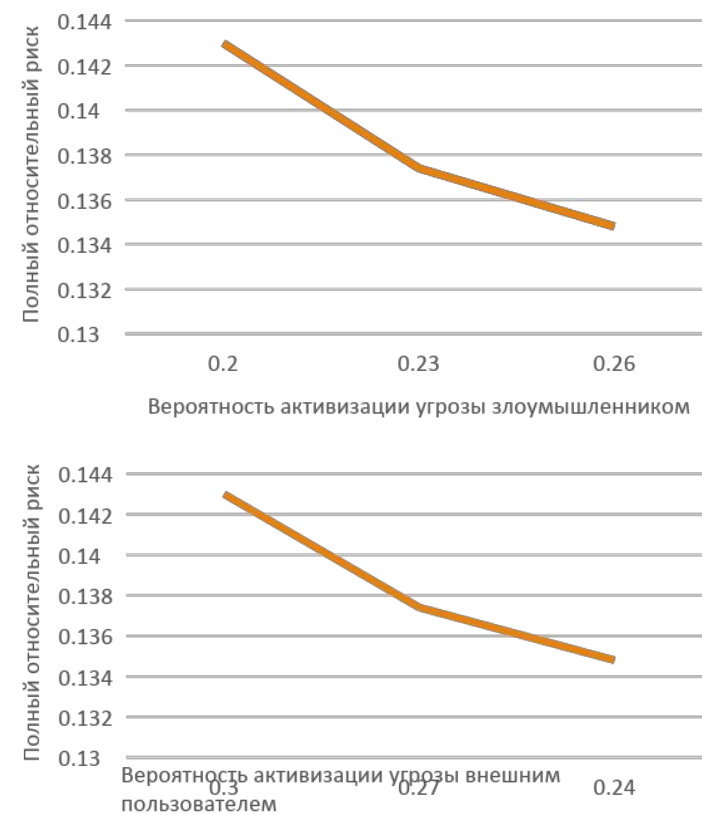


Таблица расчётов

Выводы по дипломной работе

1. Были рассмотрены особенности защиты данных: виды информационных ресурсов, основные виды атак на данные и особенности работы удаленных пользователей
2. Был проведен обзор основных средств защиты данных: антивирусы, системы обнаружения и вторжения, межсетевые экраны и VPN
3. Была разработана система защита данных для КС, предложены средства защиты
4. Был произведен расчет рисков для сети организации