



Создание системы защиты ИСПДн «Работники» ООО «Металлобаза»

Автор работы: Попов Георгий **Отчество**,
группа **КТУР-ХХ**

Руководитель работы: Костромитин **Имя Отчество**,
ДОЛЖНОСТЬ

Цели и Задачи работы

- Цель работы – создание системы защиты ПДн **работников** в ООО «Металлобаза».

- Задачи работы:

- анализ и обследование информационных систем

- выявление защищаемой информации

- определение перечня персональных данных

- разработка модели угроз безопасности

- разработка паспорта предприятия с точки зрения

ИБ

- разработка недостающих документов, регламентирующих защиту ПДн

- создание частного технического задания на проектирование системы защиты ПДн

- выбор СЗИ для ИСПДн «Работники»

- оценка проекта с экономической точки зрения

Характеристика предприятия

- ООО «Металлобаза» предоставляет услуги по обрезке и обработке металла, изготовление конструкций по индивидуальным чертежам.

Поставка и продажа металлопроката и металлоконструкций.

- ООО «Металлобаза» расположена в трёхэтажном кирпичном здании по адресу:
г. Челябинск, ул. 2-я Потребительская, д. 10

- Единственное соседнее здание с административными помещениями находится в 15 метрах от объекта



Виды защищаемой информации

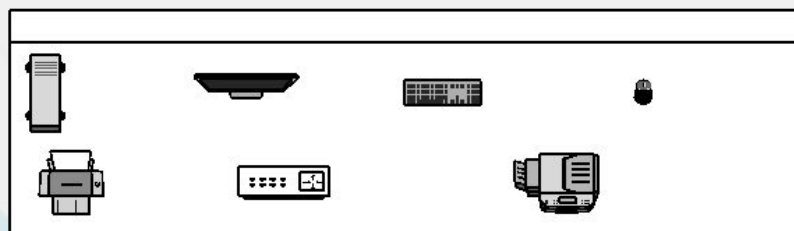
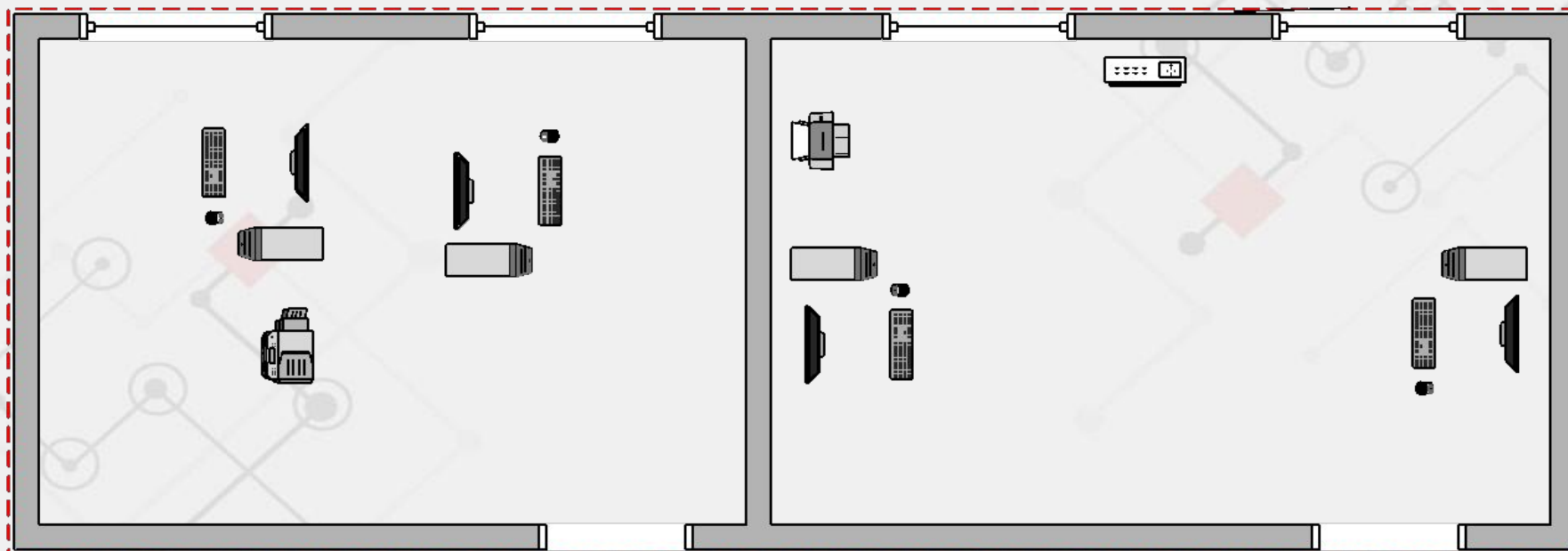
Виды защищаемой информации:

- Общедоступная информация
- Персональные данные
- Коммерческая тайна

В рамках данной ВКР, будут рассмотрены **Персональные данные работников**

Контролируемая зона

2017.01.11



Актуальные угрозы

Актуальная угроза	Меры противодействия	
	Технические	Организационные
Преднамеренные действия нарушителя	Установка и настройка сертифицированных ФСТЭК России средств защиты информации	Разработка и внедрение организационно-распорядительной документации
Непреднамеренные действия нарушителя		
Локальные уязвимости системного ПО		
Локальные уязвимости прикладного ПО		
Угрозы, реализуемые с использованием протоколов межсетевое взаимодействия		

Уровень защищенности ПДн

Категория ПДн	Специальные			Биометрические	Иные			Общедоступные			
	Нет	Нет	Да		Нет	Нет	Да	Нет	Нет	Да	
Собственные работники											
Количество субъектов	Более 100 тыс.	Менее 100 тыс.			Более 100 тыс.	Менее 100 тыс.		Более 100 тыс.	Менее 100 тыс.		
Тип актуальных угроз	1	1УЗ	1УЗ	1УЗ	1УЗ	1УЗ	2УЗ	2УЗ	2УЗ	2УЗ	2УЗ
	2	1УЗ	2УЗ	2УЗ	2УЗ	2УЗ	3УЗ	3УЗ	2УЗ	3УЗ	3УЗ
	3	2УЗ	3УЗ	3УЗ	3УЗ	3УЗ	4УЗ	4УЗ	4УЗ	4УЗ	4УЗ

- Категория ПДн - иные
- Принадлежность субъектов – работник предприятия
- Тип актуальных угроз - 3

Разработанные документы, регламентирующие безопасность ПДн

- инструкция по организации парольной защиты
- инструкция по антивирусной защите
- положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных
- инструкция пользователя информационных систем персональных данных

Антивирусное средство

Критерии	Kaspersky Endpoint Security 11	Dr.Web Enterprise Security Suite
Наличие сертификата ФСТЭК	+	+
Сертификат ФСТЭК	4068 до 22.01.2024	3509 до 27.01.2024
Общий уровень обнаружения вредоносного программного обеспечения	91.88%	92.40%
Среднее время реакции на новые угрозы, часы	6-8	6-8
Лечение активного заражения	71%	82%
Занимаемая оперативная память в обычном режиме работы, кВ	8500	8000
Время сканирования данных, мин	40-50	30-40
Стоимость, руб	19 900,00	7 800,00

Антивирусное обеспечение Dr. Web

- Сертификат соответствия № 3509 выдан ФСТЭК России 27.01.2016, действителен до 27.01.2019. Сертификат удостоверяет, что Dr.WEB Enterprise Security Suite является средством антивирусной защиты информации и соответствует требованиям документов «Требования к средствам антивирусной защиты», «Профиль защиты средств антивирусной защиты типа «А» второго класса защиты», «Профиль защиты средств антивирусной защиты типа «Б» второго класса защиты», «Профиль защиты средств антивирусной защиты типа «В» второго класса защиты», «Профиль защиты средств антивирусной защиты типа «Г» второго класса защиты».



Российский разработчик
антивирусов Dr.Web



Опыт разработки с 1992
года



Dr.Web пользуются
в 200+ странах мира



Dr.Web в Реестре
Отечественного ПО



Поставка антивируса
как услуги с 2007 года



Круглосуточная
поддержка на русском
языке

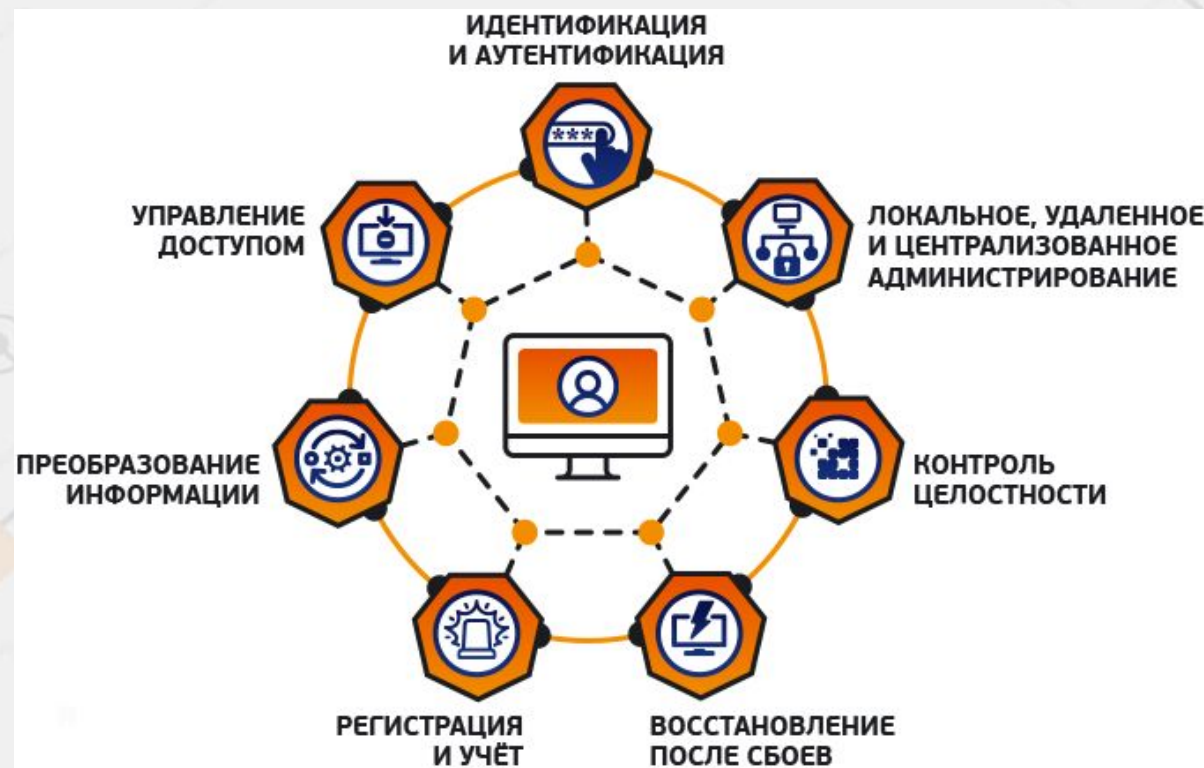


СЗИ от НСД с модулем МЭ

Критерии	Dallas Lock 8.0-K	Secret Net Studio
Наличие сертификата ФСТЭК	+	+
Сертификат ФСТЭК	2720 до 25.09.2021	3745 до 16.05.2020
Класс защищенности	По 5 классу защищенности	По 3 классу защищенности
Уровень контроля НДВ	По 4 уровню контроля	По 2 уровню контроля
Класс автоматизированных систем	До класса 1Г включительно	До класса 1Б включительно
Дополнительные аппаратные требования: свободное место на жестком	1,00 Гб	2,00 Гб
Дополнительная аппаратная поддержка	есть (СДЗ Dallas Lock)	есть (ПАК «Соболь»)
Поддержка ОС семейства Windows	+	+
Модуль межсетевое экрана	+	+
Стоимость, руб	8 500,00	9 775,00

СЗИ Dallas Lock 8.0-К

Обеспечивает показатели защищенности от НСД к информации по 5 классу защищенности СВТ и по 4 классу контроля уровня недеklarированных возможностей.



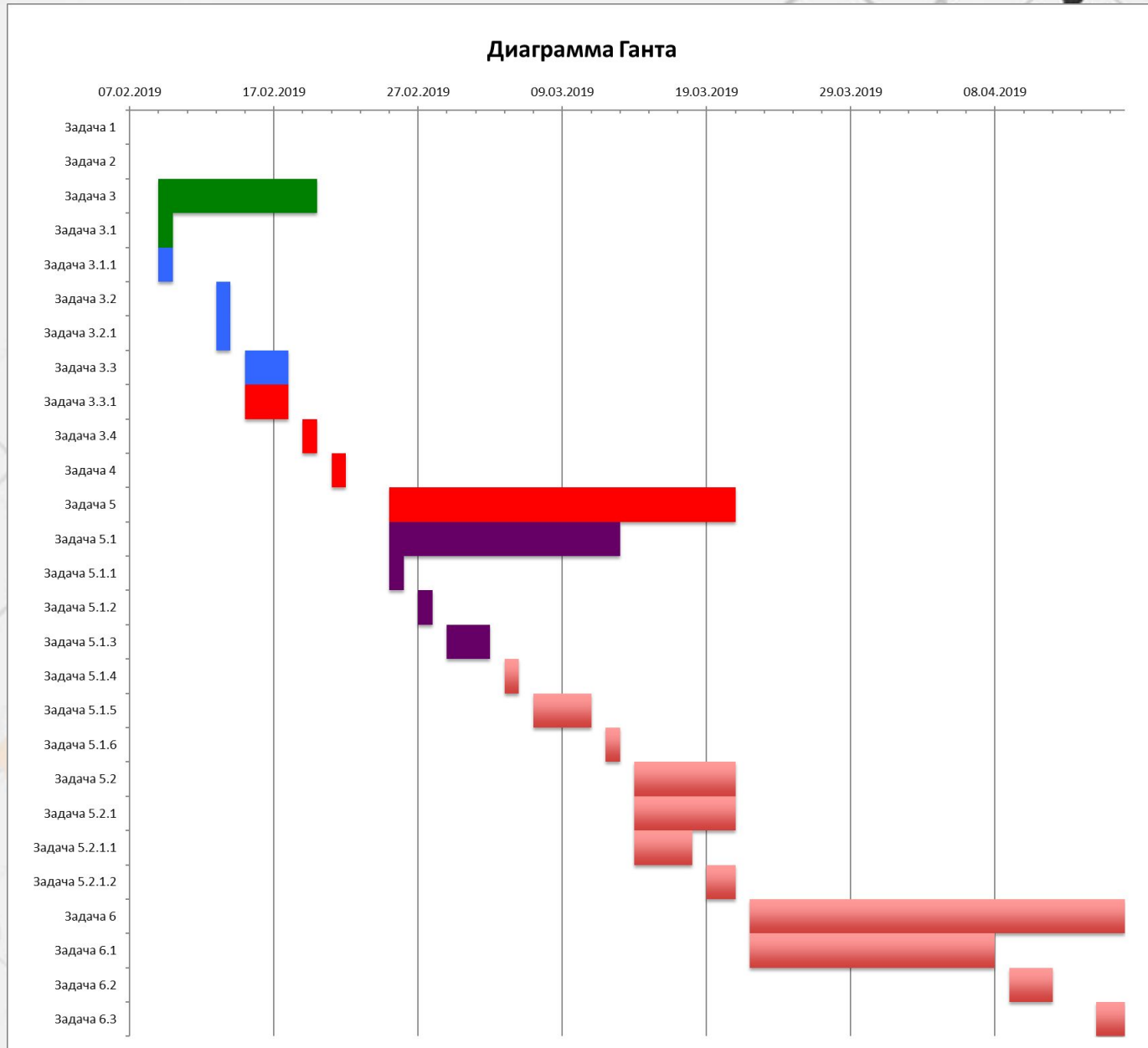
Модуль МЭ Dallas Lock 8.0-К

- Межсетевой экран (МЭ) Dallas Lock предназначен для защиты рабочих станций и серверов от несанкционированного доступа посредством осуществления контроля и фильтрации проходящих через сетевые интерфейсы ПК сетевых пакетов в соответствии с заданными правилами. Является сертифицированным модулем в составе СЗИ Dallas Lock 8.0.
- Соответствует требованиям ФСТЭК России:
Профиль защиты межсетевых экранов типа «В» четвертого класса защиты



- Возможность полного блокирования передачи данных по определенным сетевым протоколам.
- Блокировка неблагонадежных ресурсов в сети Интернет как с использованием IP-адреса, так и по URL сайта
- Гибкая настройка отдельных правил фильтрации, а также возможность выполнения групповых операций над правилами

Диаграмма Ганта



Заключение

По завершению создания системы защиты будут решены следующие основные задачи:

- проведено обследование Предприятия;
- описана существующая система защиты информации;
- проведён анализ и разработаны недостающие документы, регламентирующие безопасность ООО «Металлобаза»;
- разработан технический паспорт для ООО «Металлобаза»;
- разработана модель угроз и уязвимостей для ИСПДн «Работники»;
- был установлен уровень защищенности ИСПДн «Работники»;
- разработан проект по нейтрализации актуальных угроз информационной безопасности для ООО «Металлобаза»;
- выбраны и внедрены средства защиты информации с учетом требований руководящих документов.



Спасибо за внимание!