Содержание

1 ВВЕДЕНИЕ

Дипломную практику я проходил в ОМВД «Ивановский» УВД по Амурской области

Целями практики является:

1) Комплексное освоение всех видов профессиональной деятельности специальности «Обеспечение информационной безопасности автоматизированных систем»;

2) Формирование профессиональных компетенций;

3) Приобретение опыта практической работы.

Задачами практики является

1) Изучение и анализ соответствия нормативно-правовой базы информационной безопасности предприятия;

2) Исследование факторов, влияющих на построение КСЗИ предприятия, в том числе виды конфиденциальной информации;

3) Построение модели угроз и уязвимостей информационной системы предприятия;

4) Анализ эффективности системы защиты на предприятии;

5) Разработка направлений по совершенствованию КСЗ предприятия на основе применения мероприятий организационной, технической и программной защиты;

6) Изучение методик контроля ЗИ на предприятии.

7) Изучение работы средств ЗИ технических и программных

2 ХАРАКТЕРИСТИКА ОМВД ИВАНОВСКОГО РАЙОНА

2.1 Общие сведение

ОМВД «Ивановский» управления внутренних дел по Амурской области межмуниципальный отдел МВД России является органом исполнительной власти, осуществляющий функции по выработке и реализации политики и нормативно-правовому регулированию в сфере внутренних дел.

Почтовый адрес: 676930, с. Ивановка, район ул. Галушкина, 1.

Телефон 8(416-49)52-9-10, Факс 8(41649) 52-2-22.

Электронная почта: ivanovka.rgn@mail.ru

Основными задачами деятельности предприятия являются:

1) Обеспечение личной безопасности граждан и общественной безопасности, охрана общественного порядка и собственности;

2) Осуществление мер по предупреждению и пресечению преступлений и административных правонарушений;

3) Выявление и раскрытие преступлений, производство дознания по уголовным делам.

2.2 Сведения о Аппаратном обеспечении

В ОМВД «Ивановский» имеется следующее аппаратное обеспечение:
69 Персональных компьютеров (ПК), со следующими характеристиками:

Процессор: Core i3 43220, ОЗУ: 4gb, Твердотельные накопители: 120 Гб ssd и 500 Гб hdd, Монитор: 21.5``, Операционная система Windows 10
1 Сервер, со следующими характеристиками:

Процессор: 3.10 -3.50GHz Intel® Xeon® E3-1220V3 (Haswell) 4-Core, 8MB cache, ОЗУ: DIMM 4x8GB DDR 3, Твердотельный накопитель: 2x4000GB SATA hard drive (7200 rpm), Операционная система: MS Windows Server 2012 Standart 64-bit, RUS, 5 CAL Device.

Схематично расположение аппаратного обеспечения учреждения приведено на рисунке 1.

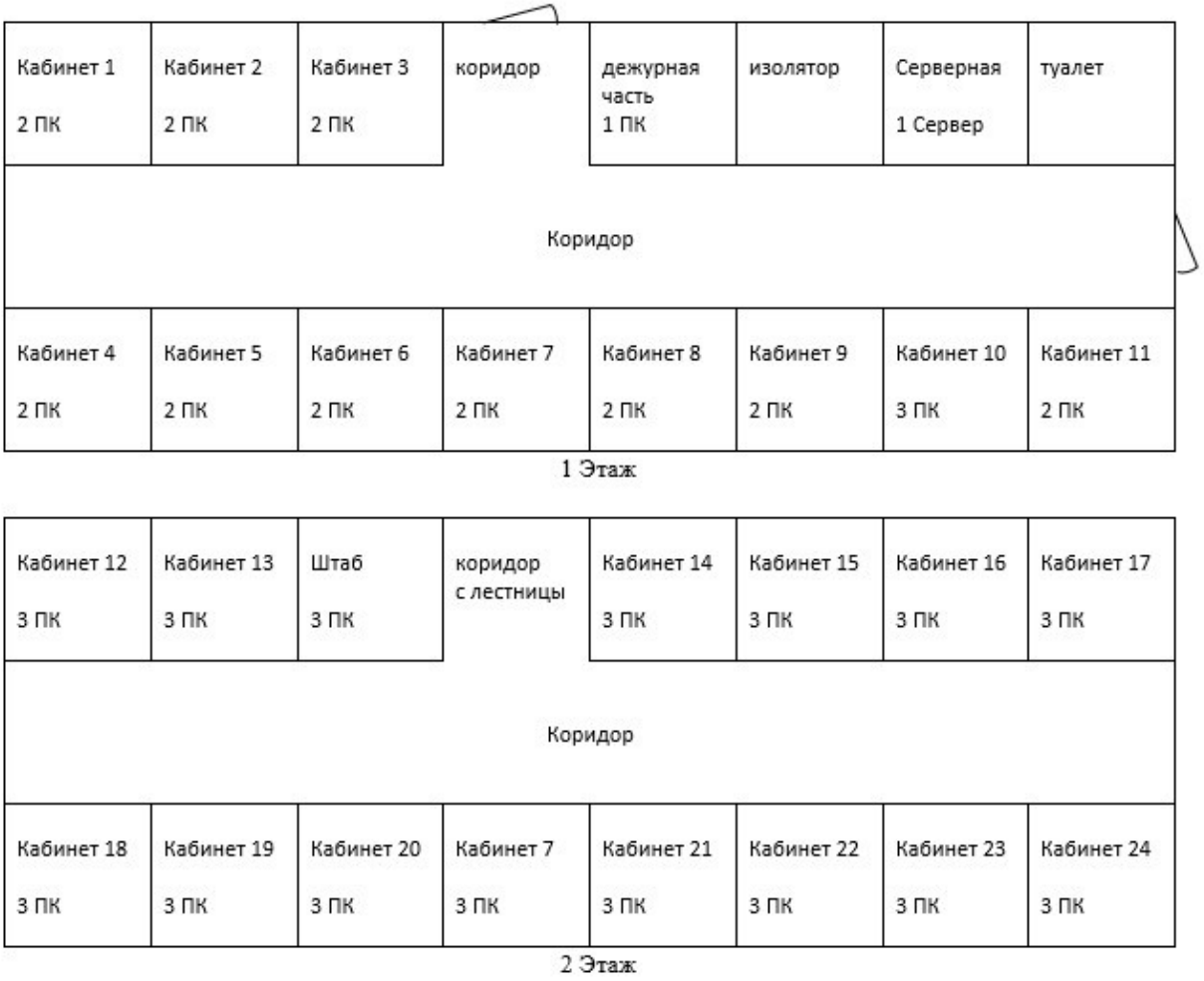

Рисунок 1 Схема расположения аппаратных средств

2.3 Сведения о программном обеспечении

В ОМВД «Ивановский» имеется следующее программное обеспечение (ПО), направленное на обеспечение информационной безопасности в автоматизированных системах МВД:

Антивирусное ПО: Kaspersky Endpoint Security

Средство защиты информации от несанкционированного доступа: Secret Net Studio

Данное ПО установлено на каждом ПК учреждения и необходимо, для обеспечения защиты данных, обрабатываемых в учреждении.

3. МОДЕЛЬ УГРОЗ И УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРЕДПРИЯТИЯ

На основе анализа информационной защиты в учреждении, а также с учетом анализа эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности была составлена модель угроз.

Модель угроз – систематизированный перечень актуальных угроз безопасности персональных данных (ПДн) при их обработке в ИСПДн.

Модель угроз необходима для выявления и учета угроз безопасности ПДн, в конкретных условиях и составляет основу планирования мероприятий, направленных на обеспечение безопасности ПДн.

Модель угроз позволяет:

- сформировать обусловленные требования по защите ПДн при их обработке в ИСПДн;
- реализовать подход по обеспечению безопасности ПДн с минимальными затратами.

Для того, чтобы рассчитать актуальные угрозы, то есть угрозы, которые могут быть реализованы в ИСПДн и представляют опасность для ПДн, необходимо рассчитать уровень исходной защищенности. Это можно представить в виде таблицы 1.

Таблица 1 – Уровень исходной защищенности

	Низкая	Средняя	Высокая
По территориальному размещению			
Локальная ИСПДн в пределах 1-го здания			+
По наличию соединения с сетями общего пользования			
ИСПДн, имеющая одноточечный выход в сеть		+	
По встроенным (локальным) операциям с записями баз ПДн			
Запись, удаление, сортировка		+	

По разграничению доступа по ПДн			
ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющиеся владельцами ИСПДн		+	
По наличию соединений с другими базами ПДн иных ИСПДн			
ИСПДн, в которой используется база ПДн, принадлежащая владельцу			+
По уровню обобщения (обезличивания)			
ИСПДн, в которой данные обезличиваются только при передаче в другие организации		+	
По объёму ПДн, которые предоставляются сторонними пользователями без предварительной обработки			
ИСПДн, не предоставляющая никакой информации			+

Уровень исходной защищенности средний, то есть Y1=5

Далее определяем частоту реализации угрозы Y2 — определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн.

Для этого показателя вводятся 4 вербальных градации: маловероятно (0), низкая вероятность (2), средняя вероятность (5), высокая вероятность (10).

Возможность реализации угрозы определяется соотношением:

$$Y = (Y1 + Y2)/20$$

Далее формируется вербальная интерпретация реализуемости угрозы следующим образом:

— низкая;

— средняя;

— высокая;

— очень высокая.

Потом оценивается опасность каждой угрозы.

Таблица 2 – Расчет актуальных угроз

№ угрозы	Частота реализации угроз Y2	Возможность реализации угроз Y	Опасность каждой угрозы	Актуальность угроз
1	Маловероятно(0)	(5+0)/20=0,25(н)	Низкая	Неактуальная
2	Маловероятно(0)	(5+0)/20=0,25(н)	Низкая	Неактуальная
3	Маловероятно(0)	(5+0)/20=0,25(н)	Низкая	Неактуальная
4	Маловероятно(0)	(5+0)/20=0,25(н)	Низкая	Неактуальная
5	Маловероятно(0)	(5+0)/20=0,25(н)	Низкая	Неактуальная
6	Маловероятно(0)	(5+0)/20=0,25(н)	Низкая	Неактуальная
7	Низкая (2)	(5+2)/20=0,35(с)	Низкая	Неактуальная
8	Маловероятно(0)	(5+0)/20=0,25(н)	Низкая	Неактуальная
9	Маловероятно(0)	(5+0)/20=0,25(н)	Средняя	Неактуальная
10	Маловероятно(0)	(5+0)/20=0,25(н)	Средняя	Неактуальная
11	Маловероятно(0)	(5+0)/20=0,25(н)	Средняя	Неактуальная
12	Средняя (5)	(5+5)/20=0,5 (с)	Средняя	Актуальная
13	Средняя (5)	(5+5)/20=0,5 (с)	Средняя	Актуальная
14	Средняя (5)	(5+5)/20=0,5 (с)	Средняя	Актуальная
15	Средняя (5)	(5+5)/20=0,5(с)	Средняя	Актуальная
16	Средняя (5)	(5+5)/20=0,5 (с)	Низкая	Неактуальная
17	Маловероятно(0)	(5+0)/20=0,25(н)	Средняя	Неактуальная
18	Маловероятно(0)	(5+0)/20=0,25(н)	Средняя	Неактуальная
19	Низкая (2)	(5+2)/20=0,35(с)	Высокая	Актуальная
20	Маловероятно(0)	(5+0)/20=0,25(н)	Средняя	Неактуальная
21	Низкая (2)	(5+2)/20=0,35(с)	Низкая	Неактуальная
22	Маловероятно(0)	(5+0)/20=0,25(н)	Средняя	Неактуальная

23	Средняя (5)	(5+5)/20=0,5 (с)	Средняя	Актуальная
24	Низкая (2)	(5+2)/20=0,35(с)	Средняя	Актуальная
25	Средняя (5)	(5+5)/20=0,5 (с)	Высокая	Актуальная
26	Средняя (5)	(5+5)/20=0,5 (с)	Высокая	Актуальная
27	Низкая (2)	(5+2)/20=0,35(с)	Средняя	Актуальная
28	Низкая (2)	(5+2)/20=0,35(с)	Низкая	Неактуальная
29	Низкая (2)	(5+2)/20=0,35(с)	Низкая	Неактуальная
30	Средняя (5)	(5+5)/20=0,5 (с)	Высокая	Актуальная
31	Средняя (5)	(5+5)/20=0,5 (с)	Высокая	Актуальная
32	Средняя (5)	(5+5)/20=0,5 (с)	Средняя	Актуальная
33	Низкая (2)	(5+2)/20=0,35(с)	Средняя	Актуальная
34	Средняя (5)	(5+5)/20=0,5 (с)	Средняя	Актуальная
35	Низкая (2)	(5+2)/20=0,35(с)	Высокая	Актуальная
36	Средняя (5)	(5+5)/20=0,5 (с)	Высокая	Актуальная
37	Низкая (2)	(5+2)/20=0,35(с)	Средняя	Актуальная
38	Низкая (2)	(5+2)/20=0,35(с)	Средняя	Актуальная
39	Низкая (2)	(5+2)/20=0,35(с)	Средняя	Актуальная
40	Низкая (2)	(5+2)/20=0,35(с)	Средняя	Актуальная
41	Средняя (5)	(5+5)/20=0,5 (с)	Высокая	Актуальная
42	Маловероятно(0)	(5+0)/20=0,25(н)	Средняя	Неактуальная
43	Маловероятно(0)	(5+0)/20=0,25(н)	Средняя	Неактуальная
44	Маловероятно(0)	(5+0)/20=0,25(н)	Средняя	Неактуальная
45	Низкая (2)	(5+2)/20=0,35(с)	Средняя	Актуальная
46	Маловероятно(0)	(5+0)/20=0,25(н)	Средняя	Неактуальная
47	Средняя (5)	(5+5)/20=0,5 (с)	Средняя	Актуальная

4. АНАЛИЗ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ В УЧРЕЖДЕНИИ

Чтобы предотвратить утечку информации в учреждении проводится инженерно-техническая защита (ИТЗ). ИТЗ — это совокупность специальных органов, технических средств и мероприятий по их использованию в целях защиты конфиденциальной информации. По функциональному назначению средства инженерно-технической защиты делятся на следующие группы:

физические средства - включают различные средства и сооружения, препятствующие физическому проникновению (или доступу) злоумышленников на объекты защиты и к материальным носителям конфиденциальной информации и осуществляющие защиту персонала, материальных средств, финансов и информации от противоправных воздействий;

аппаратные средства - сюда входят приборы, устройства, приспособления и другие технические решения, используемые в интересах защиты информации. Основная задача аппаратных средств — обеспечение стойкой защиты информации от разглашения, утечки и несанкционированного доступа через технические средства обеспечения производственной деятельности;

программные средства - охватывают специальные программы, программные комплексы и системы защиты информации в информационных системах различного назначения и средствах обработки (сбора, накопления, хранения, обработки и передачи) данных.

5 ПРИМЕНЕНИЕ ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Основным средством защиты от вирусов можно считать использование антивирусов. Антивирусное средство установленное на ПЭВМ и на почтовом сервере предприятия это «Антивирус Касперского». Предоставляет пользователю защиту от вирусов, троянских программ, шпионских программ, руткитов, adware, а также неизвестных угроз с помощью проактивной защиты, включающей компонент HIPS. Также правильная политика безопасности, включающая

обновление используемых программ и антивирусных средств, так как антивирусные средства пассивны и не в состоянии гарантировать 100 % защиту от неизвестных вирусов, поможет избежать вирусного заражения

Kaspersky Endpoint Security для Windows – это комплексное, отмеченное наградами решение, которое работает на базе новейших технологий и защищает все конечные устройства Windows и данные на них.

Вот только некоторые преимущества приложения:

1) Многоуровневая защита
2) Сочетание передовых технологий и глубокой аналитики
3) Интеграция с облачной базой данных
4) Выявление подозрительного поведения
5) Автоматическая защита от эксплойтов
6) Блокирование сетевых атак
7) Защита общих папок от шифрования

Системные требования Kaspersky Endpoint Security:

- 2 Гб свободного места на жестком диске
- Процессор Intel Pentium 1 ГГц (с поддержкой набора инструкций SSE2 или совместимый аналог)
- Оперативная память 1 Гб для ОС 32 бит (2 Гб для ОС 64 бит)
- Операционная система не ниже Windows 7

При прохождении практики мной был получен опыт работы с данным антивирусным ПО и его настройки.

На рисунках 2-4 отображен интерфейс Kaspersky Endpoint Security в момент настройки.

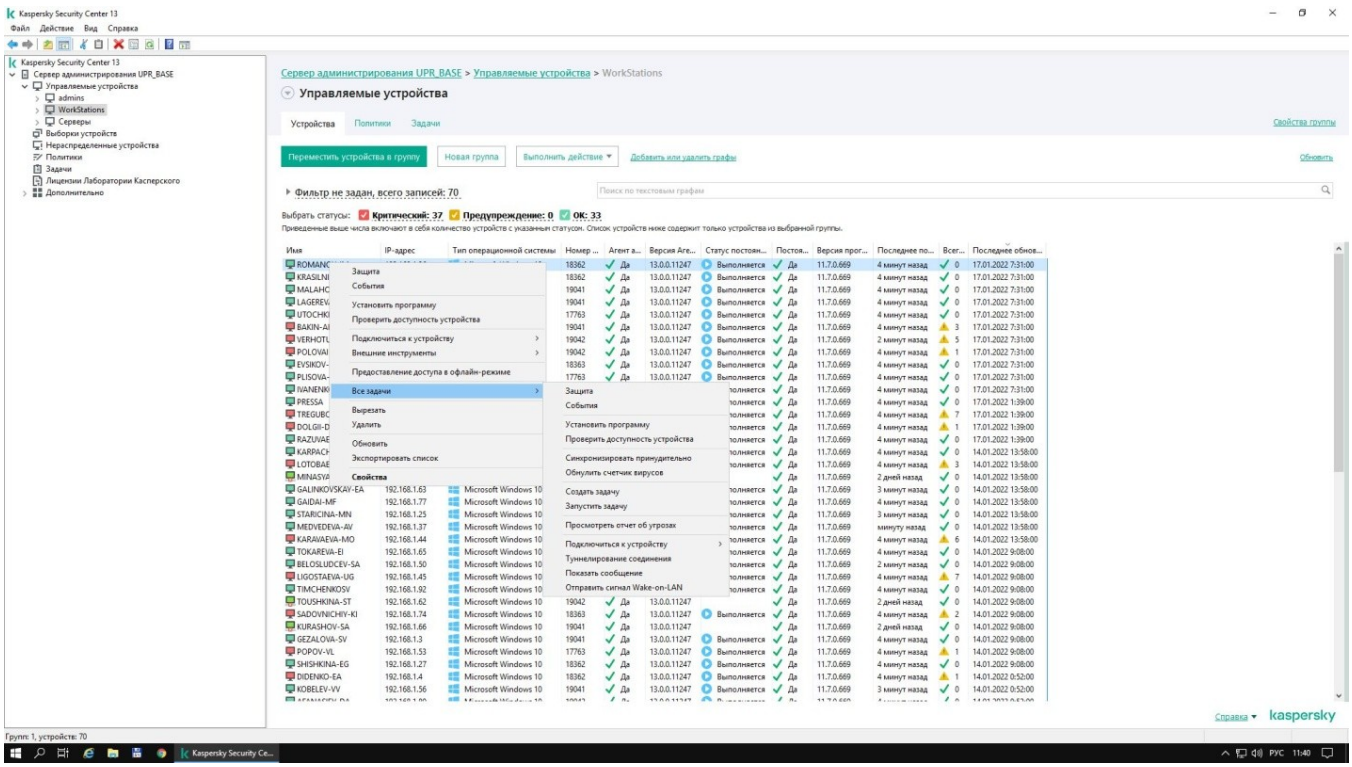

Рисунок 2– список задач Kaspersky Endpoint Security

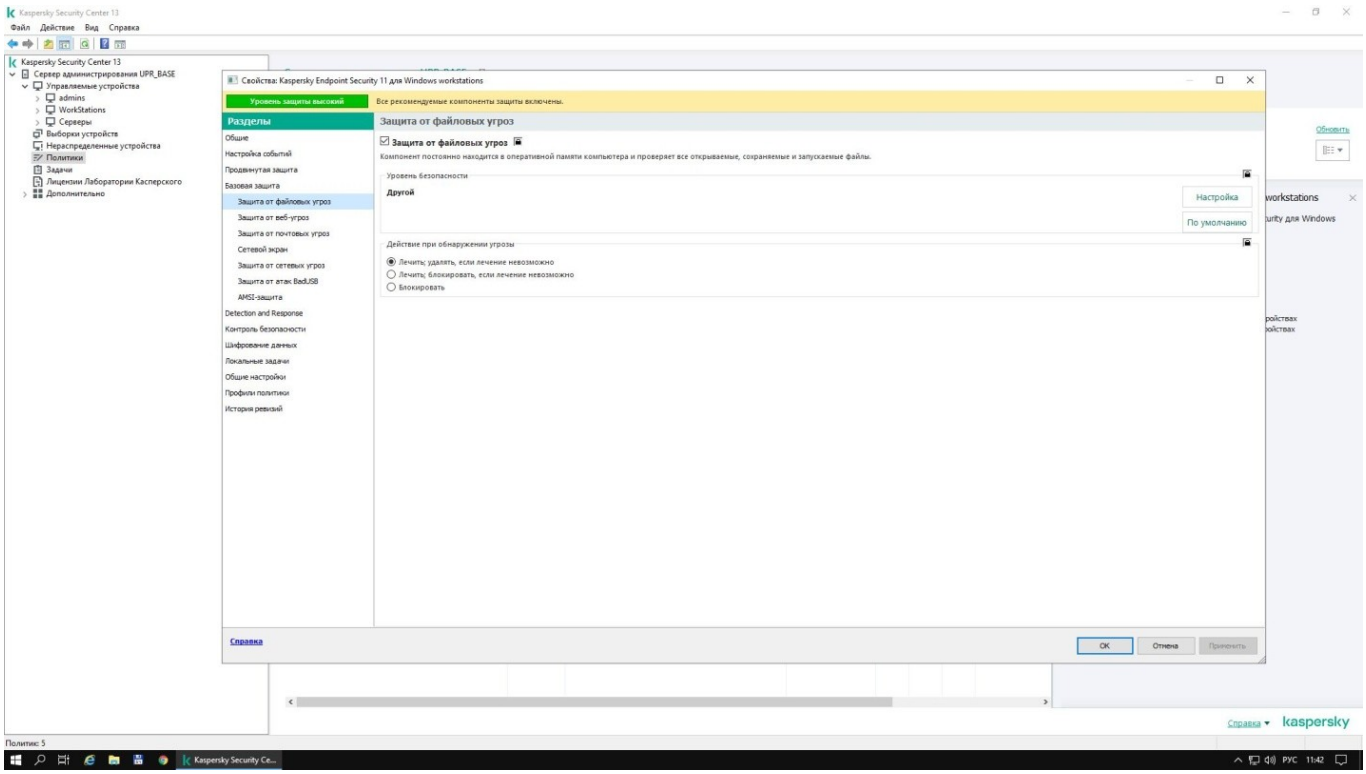

Рисунок 3– свойства Kaspersky Endpoint Security

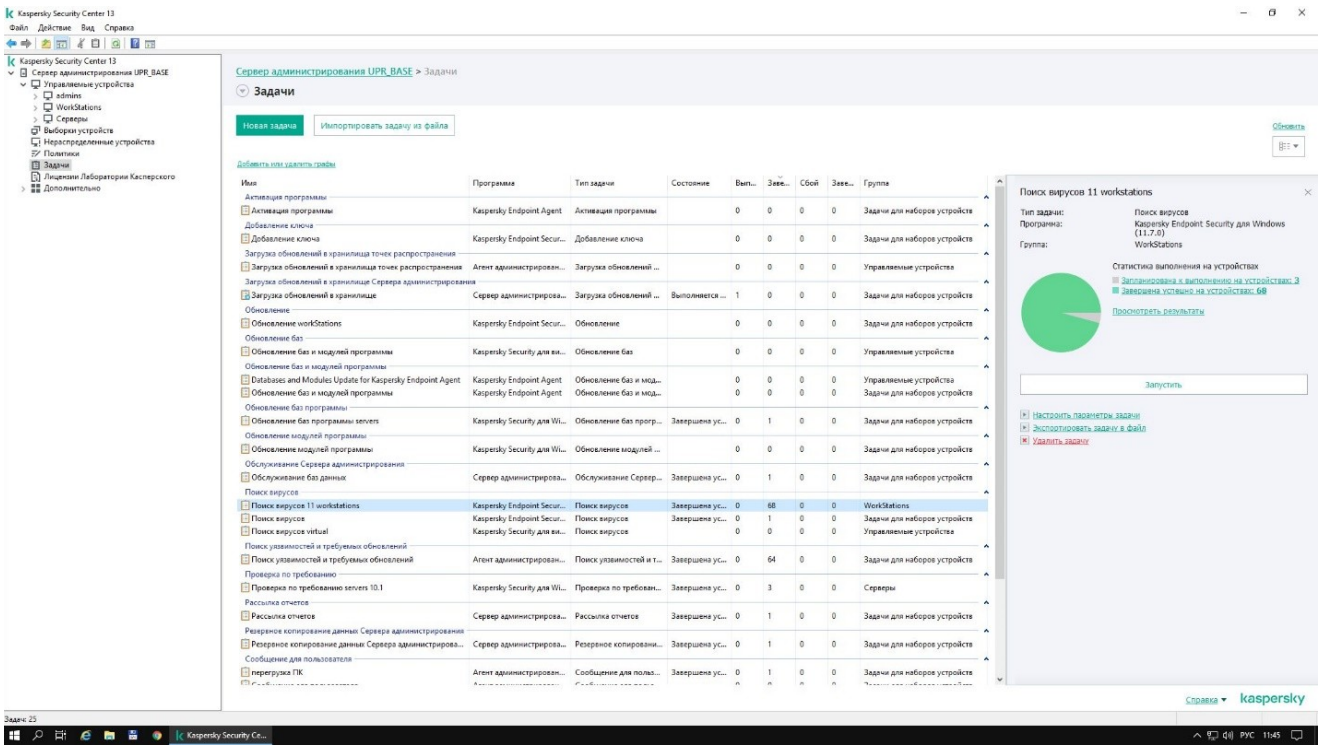

Рисунок 4– задача по поиску вирусов в центре управления Kaspersky

Secret Net Studio – является стандартом для ряда критически важных отраслей российской экономики в области защиты конфиденциальной информации, включая защиту государственной тайны.

Единая система управления продуктами для защиты Windows, Linux и платами доверенной загрузки. Система масштабируется до управления десятками тысяч рабочих станций и серверов.

Единый агент оптимально использует ресурсы компьютера для защиты от вирусов, сетевых атак, а также от несанкционированного доступа к конфиденциальным данным.

Встроенные шаблоны настроек безопасности обеспечивают и отслеживают требуемый регулятором уровень защиты ИТ-инфраструктуры с минимальными усилиями со стороны обслуживающего персонала.

Ключевые возможности СЗИ от НСД SecretNet:

- аутентификация пользователей;
- разграничение доступа пользователей к информации и ресурсам автоматизированной системы;
- доверенная информационная среда;

- контроль утечек и каналов распространения конфиденциальной информации;
- контроль устройств компьютера и отчуждаемых носителей информации на основе централизованных политик, исключающих утечки конфиденциальной информации;
- централизованное управление системой защиты, оперативный мониторинг, аудит безопасности;
- масштабируемая система защиты, возможность применения SecretNet (сетевой вариант) в организации с большим количеством филиалов.

Системные требования Secret Net Studio 8.6:

- Операционная система: не ниже Windows 7 SP1
- Процессор: в соответствии с требованиями ОС, установленной на компьютер
- Оперативная память: Минимально – 2 гБ (Рекомендуется – 4 гБ)
- Жесткий диск (свободное пространство) 4 гБ

При прохождении практики мной был получен опыт работы с данным СЗИ, его настройки и особенностей эксплуатации.

На рисунках 5-8 отображен интерфейс Secret Net Studio в момент эксплуатации.

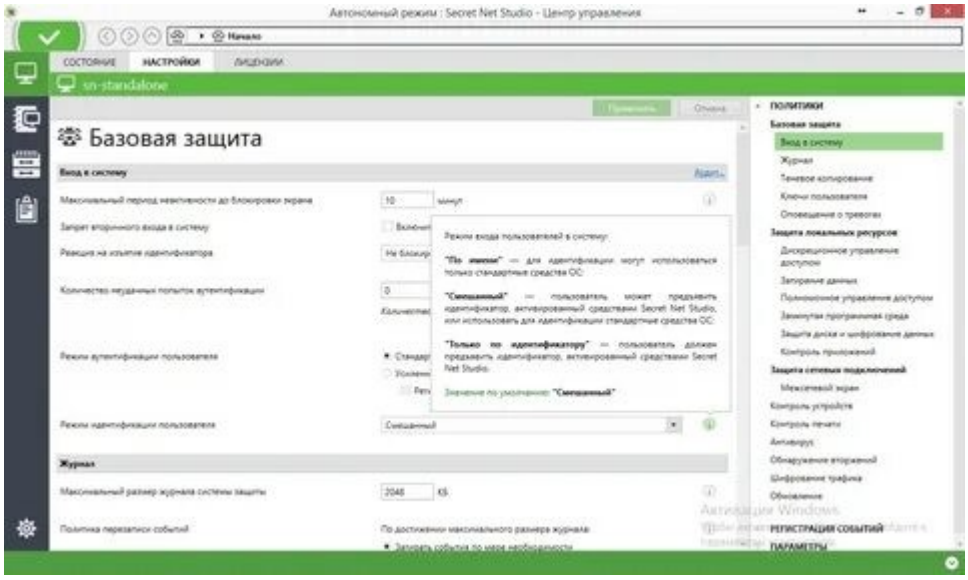

Рисунок 5- Окно настройки защиты входа в систему

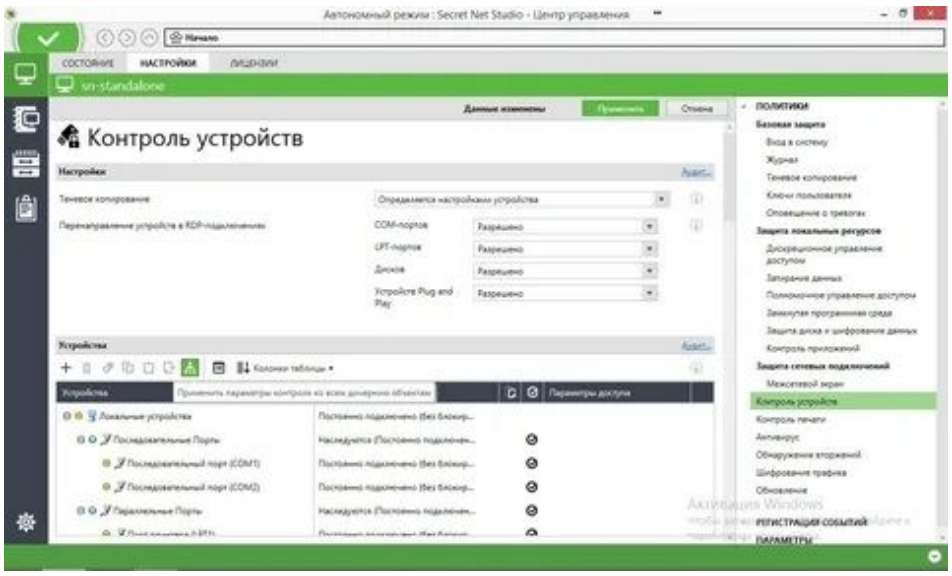

Рисунок 6-Окно настройки контроля подключения устройств

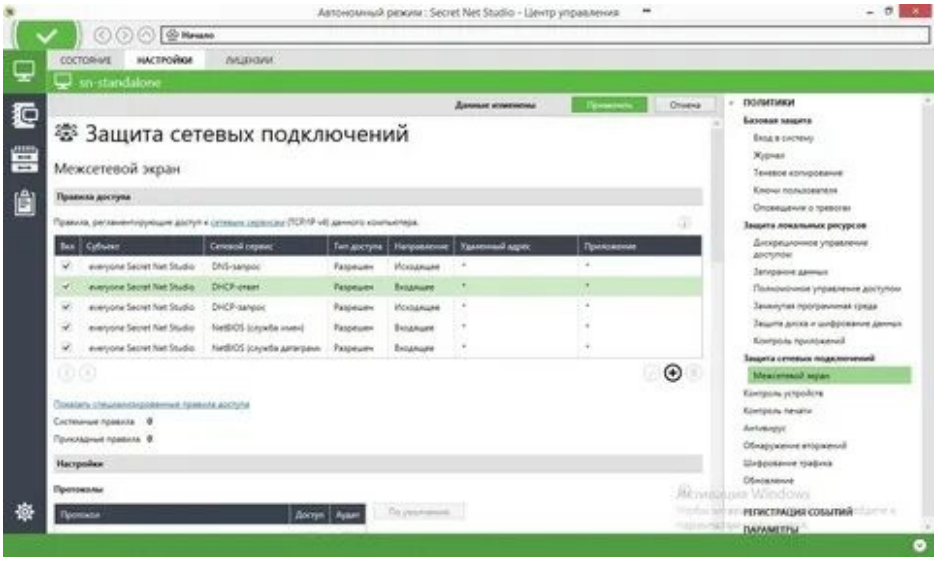

Рисунок 7-Окно настройки защиты сетевых подключений

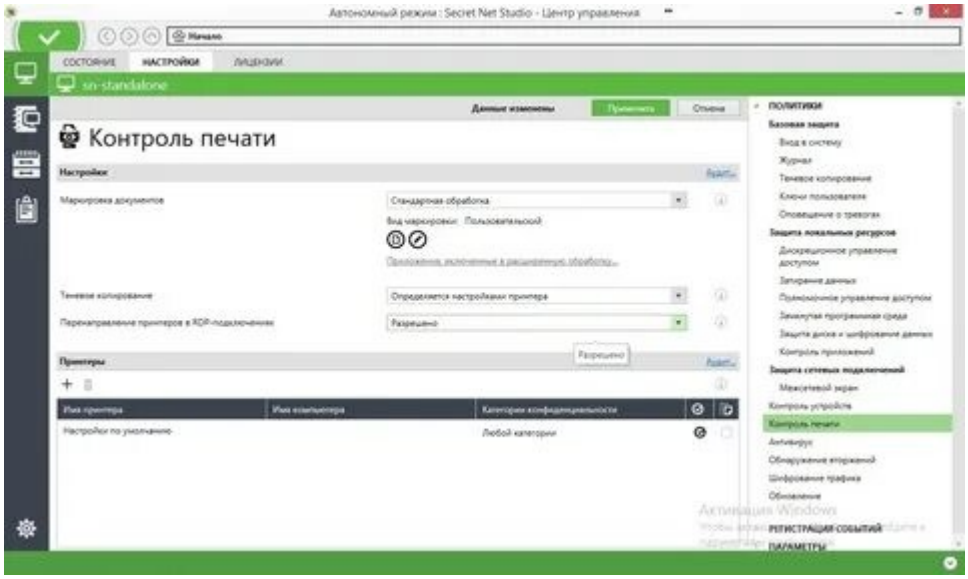

Рисунок 8-Окно настройки контроля печати

В данном отделе отлажена своя система защиты информации,

Все компьютеры на предприятии оснащены антивирусами и современной ОС, и ПО, и отлаженным FIREWALL, на всех компьютерах присутствуют пароли, все опечатаны, без специального разрешения начальника отдела защиты информации их вскрывать запрещено.;

Все коммуникации как телефонные линии так и локальные сети (оптоволоконные) защищены внешним корпусом или находятся в самой стене что снижает риск прослушивания и считывания информации путём подключения к сетям. Вся информация на предприятии хранится на сервере, в специальном защищенном помещение.

4 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

Территория всего учреждения в целом защищена от проникновения злоумышленника и техническими средствами, на предприятии также отлично организован контрольно-пропускной режим, в ОМВД существует 1 КПП, который осуществляет пропуск сотрудников и граждан с внутренней стороны здания ОМВД. Вход на территорию учреждения осуществляется со двора. На предприятии также задействованы для комплексной системы защиты информации:

1 КПП, на нём всегда присутствует видеонаблюдение, также на данном КПП присутствует сотрудник УМВД, проверяющий пропуска и открывающий доступ в здание по средствам электронной разблокировки дверей;

На всей территории УМВД присутствуют камеры, записывающие всё происходящее как внутри, так и снаружи организации, для возможного выявления злоумышленника или других угроз;

Задачи технических средств защиты:

1. защита материальных ценностей предприятия;
2. защита от несанкционированного проникновения на объект;
3. предоставление высокого статуса охраняемому объекту контрольно-пропускной режим;
4. проверка и контроль авто, въезжающих на охраняемую территорию;
5. контроль над всей территорией;

6. контроль над сотрудниками;
7. оперативное устранение аварийных обстоятельств;
8. быстрое реагирование в случае нарушения безопасности;

При организации технических средств защиты берут во внимание следующие параметры:

1. размер охраняемого объекта и его территории;
2. наличие и число локальных участков;
3. квадратура всего периметра объекта;
4. возможные риски для сотрудников и охранников;
5. степень ценности имущества на объекте и материальной ответственности охранников за нее;
6. есть ли необходимость во время работы применять различные средства связи и оружие;
7. приблизительная стратегия и план работы представителей физической охраны.

Вся эта информация и ее подробный анализ дают возможность разработать максимально надежную систему и стратегию технической защиты. Только так можно обеспечить полную безопасность охраняемого объекта и его территории. Но важно осознавать, что техническая защита является всего лишь одним из элементов охранной системы и она должна работать вместе с другими видами защиты информации, включая программные и программно-аппаратные.

На предприятии размещен турникет. Рядом с турникетом помещение дежурной части, в котором дежурный сотрудник просматривает камеры видеонаблюдения. На рисунке 12 показано местоположение турникета.

Рисунок 9 – расположения турникета

На предприятии присутствует как система видеонаблюдения, так и система пожарной сигнализации.

В систему пожарной сигнализации входят: датчики дыма, системы оповещения и управления эвакуацией.

6 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

На практике я сформировал назначение, структуру и основные характеристики ИСПДН.

Информационная система персональных данных ИСПДн предназначена для автоматизации процесса обработки персональных данных работников и обучающихся.

Рассматриваемая ИСПДн имеет подключение к сетям общего пользования посредством сертифицированного межсетевого экрана (МЭ). Защита трафика осуществляется с помощь применения средств шифрования.

Все компоненты ИСПДн находятся внутри контролируемой зоны.

Обработка персональных данных в ИСПДн ведется в многопользовательском режиме с равными полномочиями допущенных пользователей в рамках своих служебных обязанностей.

Режим обработки предусматривает следующие действия с персональными данными: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Основные параметры ИСПДн приведены в Таблице 3.

Таблица 3 – Параметры ИСПДн

Заданные характеристики безопасности персональных данных	Информационная система обрабатывает ПДн четвертого уровня защищенности
Структура информационной системы	69 АРМ и 1 сервер с подключением к сети общего пользования посредством МЭ
Подключение информационной системы к сетям общего пользования и (или) сетям международного информационного обмена	Имеется подключение к сети общего доступа. Подключение к сетям международного информационного обмена отсутствует.

Режим обработки персональных данных	Многопользовательская ИС
Режим разграничения прав доступа пользователей	Равные полномочия
Местонахождение технических средств информационной системы	Все технические средства находятся в пределах КЗ

В ИСПД обрабатываются следующие типы ПДн:

1. фамилия, имя, отчество;
2. год, месяц, дата и место рождения;
3. адрес проживания;
4. номер паспорта;
5. должность;
6. ИНН;
7. Номер страхового пенсионного свидетельства.

В ходе анализа исходных данных, в соответствии с Приказом ФСТЭК России от 18 февраля 2013 г. №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» определен Актом четвертый уровень защищённости ПДн в ИСПДн.

При входе в систему и выдаче запросов на доступ проводится аутентификация пользователей ИСПДн. ИСПДн располагает необходимыми данными для идентификации, аутентификации, а также препятствует несанкционированному доступу к ресурсам.

Из ИСПДн осуществляется вывод на печать сведений, содержащих персональные данные. Все пользователи ИСПДн имеют собственные роли. Список типовых ролей представлен в виде матрицы доступа в таблице 4.

Таблица 4 – Матрица доступа

Группа	Уровень доступа к ПДн	Разрешенные действия	Сотрудники отдела
Администратор безопасности	Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн. Обладает полной информацией о технических средствах и конфигурации ИСПДн. Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн. Имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн. Обладает правами конфигурирования и административной настройки технических средств ИСПДн.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение	Работник отдела информатизации
Операторы ИСПДн с правами записи	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн	- сбор - систематизация - накопление - хранение - уточнение - использование	специалисты

ЗАКЛЮЧЕНИЕ

Цель преддипломной практики, которая заключалась в исследовании процессов защиты информации, была достигнута. В процессе прохождения были изучены информационные системы, меры и средства для их защиты, официальные документы предприятия, нормативная и методическая документация, которые позволили решить многие поставленные задачи. В ходе прохождения преддипломной практики я ознакомился с организационной структурой, рассмотрел информационную систему обработки персональных данных, построил для неё модель угроз и модель нарушителя, определил класс и тип и рассчитал актуальные угрозы ИСПДн. Также ознакомился с новыми программными средствами обеспечения безопасности информации. Осмотрел различное оборудование и получил краткую характеристику по каждому из них. В процессе прохождения практики я влился в рабочий коллектив, почувствовал весь рабочий процесс предприятия.

Немаловажным является тот факт, что в процессе прохождения преддипломной практики были получены новые теоретические и практические знания в области информационной безопасности, которые несомненно будут использованы при написании дипломной работы:

- Исследование организационной структуры предприятия, выявление видов конфиденциальной информации и ресурсов.
- Обоснование актуальных угроз и определение нарушителей информационных процессов в системе организации.
- Исследование способов защиты информационных ресурсов в системе.
- Анализ каналов утечки информации на предприятии.
- Формулировка выводов о состоянии комплексной системы защиты информации в организации.

Во время прохождения практики, я сделал вывод, что состояние защищенности ОМВД Ивановского района на высоком уровне.

Исходя из всего вышеизложенного, можно сделать выводы, что все поставленные на преддипломную практику цели и задачи были выполнены.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. Приказ Федеральной службы по техническому и экспортному контролю от 5 февраля 2010 г. № 58 “Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных”
2. Приказ ФСТЭК России от 11 февраля 2013 г. N 17 Об утверждении требований о защите информации
3. Руководящий документ. Решение председателя Гостехкомиссии России от 25 июля 1997 г. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.
4. Методический документ. Методика оценки угроз безопасности информации URL: https://docs.cntd.ru/document/607699443
5. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. – М.: Форум, 2018. – 256 с.
6. Гришина, Н.В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. – М.: Форум, 2017. – 159 с.
7. Kaspersky Endpoint Security URL: https://www.kaspersky.ru/small-to-medium-business-security/endpoint-select
8. Secret Net Studio URL: https://www.securitycode.ru/products/secret-net-studio/
9. Информационная безопасность URL: https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C
10. Сайт ОМВД «Ивановский» URL: http://ivanovskiy28.ru/otdel-polizii/omvd-rossii-po-ivanovskomu-rajonu/