Министерство образования и науки Российской Федерации
Филиал Федерального государственного автономного образовательного учреждения
высшего образования
«Южно-Уральский государственный университет»
(национальный исследовательский университет)
в г. Нижневартовске

Кафедра «Информатика»

РАБОТА ПРОВЕРЕНА

РЕЦЕНЗЕНТ
Программист 1С ООО «Перспектива»
_____/М.С. Астахов_____
«_____»_____

ДОПУСТИТЬ К ЗАЩИТЕ

И.о.зав.кафедрой «Информатика»
к.ф.-м.н., доцент
_____/А.В.Ялаев_____
«_____»_____

Конфигурирование и защита сети от несанкционированного доступа

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ-09.03.01.2018.359.ПЗ ВКР

Консультанты
Экономическая часть
к.э.н., доцент
_____/А.В.Прокопьев_____
«_____»_____

Безопасность жизнедеятельности
к.ф.-м.н., доцент
_____/ А.В.Ялаев_____
«_____»_____

Руководитель работы
преподователь
_____/Р.Ф. Минханов_____
«_____»_____

Автор работы
обучающийся группы НвФл-526
_____/ С.С. Шестаков_____
«_____»_____

Нормоконтролер
старший преподаватель
_____/ Л.Н.Буйлушкина_____
«_____»_____

Нижневартовск 2018

АННОТАЦИЯ

Шестаков С.С Конфигурирование и защита сети от несанкционированного доступа – Нижневартовск: филиал ЮУрГУ, Информатика: 2018, 74 с., 14 ил., 21 табл., библиогр. список – 22 наим., 1 прил.

В данной выпускной квалификационной работе описывается процесс внедрения программно-аппаратного комплекса средств защиты информации для предприятия ООО «СЦСО Надежда». Представлен анализ предметной области исследования. Приведен литературный обзор. Представлен проект по внедрению средств защиты информационной системы предприятия, отвечающий требованиям заказчика. Рассмотрены вопросы экономической эффективности и безопасности работы.

Н.контр.	*Буйлушкина Л.Н.*			ванного доступа	«ЮУрГУ (НИУ)» в г. Нижневартовске кафедра «Информатика»
Утвердил	*Ялаев А.В.*				

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Развитие современных информационных технологий сопровождается ростом числа компьютерных преступлений и связанных с ними хищений информации, а также материальных потерь.

26 января 2007 года вступил в силу Федеральный закон «О персональных данных» № 152-ФЗ, регулирующий отношения, связанные с обработкой персональных данных (далее – ПДн), и устанавливающий требования к защите таких данных [17].

Требования закона распространяются на все государственные и коммерческие организации, в которых обрабатывается информация, попадающая под определение ПДн.

В выпускной квалификационной работе (далее – ВКР) ставится цель – защитить корпоративную сеть на предприятии ООО «СЦСО Надежда» от несанкционированного доступа на базе сертифицированных программно-аппаратных продуктов удовлетворяющих требованием регуляторов ФСТЭК и ФСБ в области защите информации. Так как в настоящее время корпоративная сеть данного предприятия не отвечает требованием ФЗ № 152 от 26 января 2007 года руководство рассматриваемой компании приняло решение организовать защиту информационной системы в соответствии с принятыми законодательными требованиями [17].

Для этого в рамках данной ВКР должны быть решены следующие задачи:

1) исследовать корпоративную сеть предприятия ООО «СЦСО Надежда»;
2) проанализировать нормативные акты средств защиты информации (далее – СЗИ);
3) рассмотреть предоставленные на рынке СЗИ;

4) осуществить пуско-наладку программно-аппаратного комплекса от несанкционированного доступа с учетом нормативных актов;

5) рассчитать экономическую целесообразность;

6) описать основные нормы безопасности работы с СЗИ.

ВКР состоит из введения, четырех разделов, заключения и приложений.

1 АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ ИСЛЕДОВАНИЯ

1.1 Обзор деятельности предприятия ООО «СЦСО Надежда»

Салон оргтехники ООО «СЦСО Надежда» – это комплекс подразделений, предоставляющих целый спектр IT услуг. Компания реализует офисную инфраструктуру офиса: поставка необходимой техники, подключение оргтехники, сетевого оборудование, телефонии, настройка программного обеспечения, оптимизация его под нужды конкретной компании.

Помимо торговли Салон оргтехники ООО «СЦСО Надежда» также оказывает услуги по эксплуатации оргтехники:

– Любой ремонт системных блоков.

– Модернизация системного блока персонального компьютера.

– Экспертная оценка состояния оргтехники.

– Отправка гарантийного и не гарантийного оборудования в специализированные сервисные центры для проведения ремонтных и профилактических работ.

– Подключение периферийного оборудования.

– Проектирование и установка локальных вычислительных сетей (далее – ЛВС).

– Администрирование серверов и рабочих станций.

– Установка и настройка лицензионного программного обеспечения.

1.2 Структура компании ООО «СЦСО Надежда».

В сервисном центре ООО «СЦСО Надежда» существуют следующие подразделения:

1. отдел «Разработки прикладного программного обеспечения»;
2. отдел «Разработки web-сайтов «под ключ»;
3. отдел «Защиты информации от несанкционированного доступа».

Рассмотрим функциональные задачи структурных подразделений ООО «СЦСО Надежда».

1) Отдел «Разработки прикладного программного обеспечения:

Оказывает услуги по внедрению и сопровождению программно-аппаратных комплексов на базе «1С: Предприятие 8. Учет в управляющих компаниях ЖКХ, ТСЖ и ЖСК», производит интеграцию программы в другие продукты 1С, в частности «1С: Бухгалтерия 8».

Салон оргтехники «Надежда» является участником целевой городской программы «Электронный муниципалитет».

2) Отдел «Разработки Web-сайтов «под ключ»:

Дизайн и программирование, регистрация домена в зоне «.ru», организация корпоративной сети электронной почты и их сопровождение.

3) Отдел «Защиты информации от несанкционированного доступа»

Специалисты предприятия проводят аудит информационных систем операторов, на основании которого заказчики могут правильно оценить состояние защищённости объектов информатизации и своевременно принять меры.

– Защита персональных данных.
– Аттестация объектов информатизации.
– Электронная подпись для участия в торгах и отчетность.
– Поставка средств защиты информации.

Установка и настройка оборудования и ПО, а также доставка и установка расходных материалов с выездом на место эксплуатации.

В настоящее время в стране большое значение уделяется защите персональных данных граждан, которые обрабатываются различными операторами. По 152-ому федеральному закону оператор, обрабатывающий персональные данные граждан, обязан их защитить в соответствии с действующим законодательством [17]. ООО «СЦСО Надежда» оказывает услуги в сфере технической защиты конфиденциальной информации на основании лицензии Федеральной службы по техническому и экспортному контролю Российской Федерации (далее – ФСТЭК).

1.3 Анализ существующей сети предприятия ООО «СЦСО Надежда»

1.3.1 Состав сети предприятия

Соединения локально вычислительной сети (далее – ЛВС) устанавливаются согласно ГОСТу 29099-91 «Сети вычислительные локальные» [16].

Коммутаторы позволяют за счет сегментации повысить производительность сети. Помимо разделения сети на мелкие сегменты, коммутаторы дают возможность создавать логические сети и легко перегруппировывать устройства в них.

Почтовый сервер mail.nadezhda-nv.ru служит для передачи сообщения от одного компьютера к другому.

Ftp-сервер выполняет функцию сетевого хранилища файлов, а также использует различных механизмы обеспечения безопасности (разграничение доступа, контроль версий файлов, резервирование информации и др.).

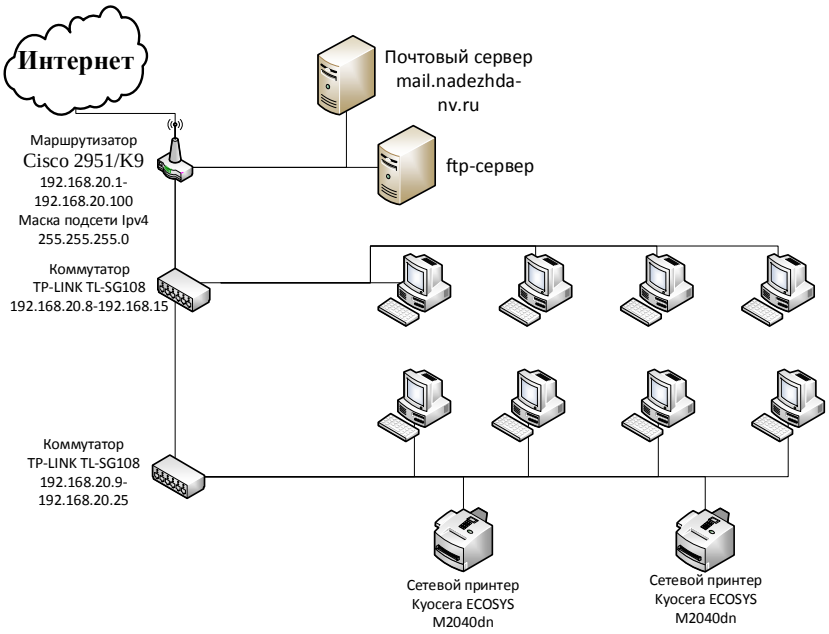


Рисунок 1.1 – Схема ЛВС предприятия ООО «СЦСО Надежда»

Корпоративная сеть предприятия ООО «СЦСО Надежда» основаны на принципе клиент-сервер, в соответствии с которым действия по обработке информации, необходимые для выполнения конкретной задачи, разделены между компьютерами, выполняющими функции клиентов или серверов.

Представлены технические характеристики оборудования компании ООО «СЦСО Надежда».

Таблица 1.1 – Технические характеристики сервера

Наименование	Комплектующие	Характеристики/модель
Сервер Fujitsu PR TX100S3P	Центральный процессор	IntelXeonE3-1220 v2
	Оперативная память	16гб/DDR3/2350 МГц
	Блок питания	1x 550 Вт
	HDD	2x2 ТБ

Серверная операционная система – Windows Server 2008 R2.

Таблица 1.2 – Технические характеристики рабочих станций

Наименование	Комплектующие	Характеристики/модель
Моноблок Lenovo C20-00 19.5"	Центральный процессор	Celeron J3060D
	Оперативная память	2 гб/DDR3/2480 МГц
	HDD	SATA 500 ГБ
	Видеосистема	Intel HD Graphics 400
Компьютер Acer Extensa EX2610G	Центральный процессор	Celeron J3060D
	Оперативная память	2гб/DDR3/2480 МГц
	HDD	SATA 500 ГБ
	Видеосистема	Intel HD Graphics 400

Маршрутизатор Cisco 2951/K9.

Таблица 1.3 – Технические характеристики маршрутизатора

Наименование	Комплектующие	Характеристики/модель
Cisco 2951/K9	WAN портов	1
	Тип WAN портов	10/100/1000Base-TX (1000 мбит/с) FPS
	Количество LAN портов	1x 550 Вт
	Протоколы Ethernet	IEEE 802.3, IEEE 802.3ab, IEEE 802.3u

Принтер многофункциональное устройство (далее – МФУ).

Таблица 1.4 – Технические характеристики принтера МФУ

Наименование	Комплектующие	Характеристики/модель
Kyocera ECOSYS M2040dn	Устройство	Принтер / сканер / копир
	Скорость печати	40 стр/мин (ч/б А4)
	Процессор	800 МГц
	Память	512 Мб, максимальный 1536 Мб
	Интерфейс	Ethernet (RJ-45), USB 2.0

Коммутатор.

Таблица 1.5 – Технические характеристики коммутатора

Наименование	Комплектующие	Характеристики/модель
TP-LINK TL-SG108	Количество портов коммутатора	8 x Ethernet 10/100/1000 Мбит/сек
	Тип управления	неуправляемый
	Поддержка стандартов	Auto MDI/MDIX, Jumbo Frame, IEEE 802.1p (Priority tags

1.3.2 Ситуация на предприятии с СЗИ

ПК расположенные в здании, объединены в доменную сеть. Доступ осуществляется доменной политикой логин / пароль требования к паролю не менее 6 символов, регулярная смена пароля не предусмотрена. У трех сотрудников компании есть полные права доступа, в связи с требованиями федерального закона «О персональных данных» № 152-ФЗ, принято решение о модернизации СЗИ [17].

1.4 Основные понятия и определения нормативных актов

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Информационная безопасность – многогранная, многомерная область деятельности, в которой успех может принести только системный, комплексный подход. Спектр интересов субъектов, связанных с использование информационных систем, можно разделить на следующие категории: обеспечение доступности, целостности и конфиденциальности информационных ресурсов и поддерживающей инфраструктуры.

Доступность – это гарантия получения требуемой информации или информационной услуги пользователем за определенное время.

Целостность – это актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

Конфиденциальность – это защита от несанкционированного доступа к информации.

Система защиты информации, как и любая система, должна иметь определенные виды собственного обеспечения (совокупность обеспечивающих подсистем), опираясь на которые она будет выполнять свою целевую функцию. В частности, СЗИ может иметь:

– Правовое обеспечение. В эту группу входят нормативные документы, положения, инструкции, руководства, требования которых являются обязательными в рамках сферы их действия.

– Организационное обеспечение. Реализация защиты информации осуществляется определенными структурными единицами, такими как: служба защиты документов; служба режима, допуска, охраны; служба защиты информации техническими средствами; информационно-аналитическая служба и другими.

– Аппаратное обеспечение. Предполагается широкое использование технических средств, как для защиты информации, так и для обеспечения деятельности самой СЗИ.

– Информационное обеспечение. Оно включает в себя сведения, данные, показатели, параметры, лежащие в основе решения задач, обеспечивающих функционирование системы. В эту группу входят как показатели доступа, учета, хранения, так и системы информационного обеспечения расчетных задач различного характера, связанных с деятельностью службы обеспечения безопасности.

– Программное обеспечение. К нему относятся различные информационные, учетные, статистические и расчетные программы, обеспечивающие оценку наличия и опасности различных каналов утечки и путей несанкционированного проникновения к источникам конфиденциальной информации.

– Математическое обеспечение. Предполагает использование математических методов для различных расчетов, связанных с оценкой опасности технических средств злоумышленников, зон и норм необходимой защиты.

– Лингвистическое обеспечение. Совокупность специальных языковых средств общения специалистов и пользователей в сфере защиты информации.

– Нормативно-методическое обеспечение. Сюда входят нормы и регламенты деятельности органов, служб, средств, реализующих функции защиты информации, различного рода методики, обеспечивающие деятельность пользователей при выполнении своей работы в условиях жестких требований защиты информации.

Под системой безопасности будем понимать организованную совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих защиту жизненно важных интересов личности, предприятия и государства от внутренних и внешних угроз. Как и любая система, система информационной безопасности имеет свои цели, задачи, методы и средства деятельности, которые согласовываются по месту и времени в зависимости от условий. На рисунке 1.2 представлена концептуальная модель безопасности информации.

Рисунок 1.2 – Концептуальная модель безопасности информации

Нормативно-правовые акты по информационной безопасности:

– Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 25.11.2017) «Об информации, информационных технологиях и о защите информации» [16].

– Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [18].

1.5 Анализ средств защиты информации

1.5.1 InfoWatch Endpoint Security

– Непрерывный мониторинг использования ИТ-ресурсов компании.

– Максимальная автоматизация «рутинных» задач ИТ и правил безопасности.

– Защита бизнеса от финансовых потерь [4].

Системные требования

Операционная система (далее – ОС): Windows Server 2000, 2008, 2010, 2012, 2016, Windows XP, Vista, 7, 8, 10.

Поддерживаемые LDAP-каталоги: Microsoft Active Directory, Novell eDirectory 4.91 SP2 и выше, Custom Directory.

СУБД: SQL Server 2005-2016 (включая Express Edition), MSDE MySQL версии 5.0 и выше (требуется ODBC).

Оперативная память: 512 MB RAM.

Свободное место на диске: 100 MB.

Стоимость продукта InfoWatch Endpoint Security: 3 736,29 руб.

1.5.2 Dallas Lock 8.0

Система защиты конфиденциальной информации от несанкционированного доступа в процессе её хранения и обработки. АРМ (применима для сложных сетевых инфраструктур) [5].

Системные требования:

СЗИ Dallas Lock 8.0 может быть установлена на персональные компьютеры, портативные и мобильные ПК (ноутбуки и планшетные ПК), серверы (файловые, контроллеры домена, терминального доступа) и виртуальные машины, работающие как в автономном режиме, так и в составе локально-вычислительной сети.

Поддерживаемые ОС:

- windows XP (SP 3) (Professional, Home, Starter);
- windows Server 2003 (R2) (SP 2) (Web, Standard, Enterprise, Datacenter);
- windows Vista (SP 2) (Ultimate, Enterprise, Business, Home Premium, Home Basic, Starter);
- windows Server 2008 (SP 2) (Standard, Enterprise, Datacenter, Web Server 2008, Storage Server 2008);
- windows 7 (SP 1) (Ultimate, Enterprise, Professional, Home Premium, Home Basic, Starter);

– windows Server 2008 R2 (SP 1) (Foundation, Standard, Web, Enterprise, Datacenter);

– windows 8 (Core, Pro, Enterprise);

– windows Server 2012 (Foundation, Essentials, Standard, Datacenter);

– windows 8.1 (Core, Pro, Enterprise);

– windows Server 2012 (R2) (Foundation, Essentials, Standard, Datacenter);

– windows 10 (Enterprise, Education, Pro, Home) и Windows 10 Creators Update;

– windows Server 2016.

Стоимость продукта Dallas Lock 8.0: 7 500,00 руб.

1.5.3 СЗИ ПАК «Соболь»

Электронный замок «Соболь» может быть использован для того, чтобы:

– доступ к информации на компьютере получили только те сотрудники, которые имеют на это право;

– в случае повреждения ОС или важных информационных массивов, хранящихся на компьютере, администратор мог вовремя принять меры по восстановлению информации [12].

Системные требования

Таблица 1.4 – Требования СЗИ ПАК «Соболь»

Операционные системы семейства Windows	Windows 8; Windows 7/7 x64 Edition; Windows Server 2012; Windows Server 2008/Server 2008 x64 Edition/Server 2008 R2; Windows Server 2003/Server 2003 x64 Edition/Server 2003 R2/Server 2003 R2 x64 Edition
Файловая система	NTFS, FAT32, FAT16, UFS2, UFS, EXT4, EXT3, EXT2
Оперативная память	В соответствии с требованиями операционной системы, установленной на компьютер
Жесткий диск	Минимально 50 Мб свободного пространства
Системная плата	Наличие свободного разъема системной шины стандарта PCI/PCI Express / Mini PCI Express. Для реализации механизма сторожевого таймера наличие хотя бы одного из разъемов: • разъем Reset; • 20 или 24-контактный разъем питания стандарта ATX

Стоимость продукта ПАК «Соболь»: 12 635,00 руб.

1.5.4 Secret Net Studio 8.2

Комплексная защита на пяти уровнях: защита данных, приложений, сетевого взаимодействия, операционной системы и работы с периферийным оборудованием [12].

– Гибкие возможности по настройке системы защиты и созданию сценариев защиты на стыке разных технологий.

– Интеграция защитных механизмов для повышения общего уровня защищенности рабочих станций и серверов.

– Создание централизованных политик безопасности и их наследование в распределенных инфраструктурах.

– Поддержка иерархии и резервирования серверов безопасности в распределенных инфраструктурах.

– Встроенная система корреляции и приоритизации событий безопасности.

Системные требования

Таблица 1.5 – Требования Secret Net Studio 8.2

Операционная система	Windows 10 (начиная с 8.1.721.0); Windows 8/8.1; Windows 7 SP1; Windows Vista SP2; Windows Server 2012/Server 2012 R2; Windows Server 2008 SP2/Server 2008 R2 SP1. Поддерживаются 32 и 64-разрядные версии ОС с установленными пакетами обновлений не ниже указанных
Процессор	В соответствии с требованиями ОС, установленной на компьютер
Оперативная память	Минимально – 2 Гб; Рекомендуется – 4 Гб
Жесткий диск (свободное пространство)	4 ГБ

Стоимость продукта Secret Net Studio 8.2: 7 343,00. руб.

1.5.5 ViPNet Client 4.3

Предназначен для защиты рабочих мест корпоративных пользователей. ViPNet Client надежно защищает от внешних и внутренних сетевых атак за счет фильтрации трафика. Кроме того, ПК ViPNet Client обеспечивает защищенную ра-

боту с корпоративными данными через зашифрованный канал, в том числе для удаленных пользователей [6].

Поддерживаемые операционные системы:

– windows Vista (32/64-разрядная);
– windows Server 2008 (32/64-разрядная);
– windows Server 2008 R2 (64-разрядная);
– windows Small Business Server 2008 (64 разрядная);
– windows Small Business Server 2008 SP2 (64-разрядная);
– windows 7 (32/64-разрядная);
– windows 8 (32/64-разрядная);
– windows 8.1 (32/64-разрядная);
– windows Small Business Server 2011 (64 разрядная);
– windows Server 2012 (64-разрядная);
– windows Server 2012 R2 (64-разрядная);
– windows 10 (32/64 разрядная).

Стоимость продукта Vipnet Client 4.3: 7 790,00 руб.

1.5.6 Анализ сравнения СЗИ

Принято решение использовать для защиты комплекс СЗИ таких как:

1. ПАК «Соболь»;
2. Secret Net Studio 8.2
3. Vipnet Client 4.3

Вследствие того, что внедрение позволит выполнить все требования Федерального закона «О персональных данных» № 152-ФЗ [17].

1.6 Основные требования предприятия к корпоративной сети передачи данных

ТРЕБОВАНИЯ

При построении информационной системы, владелец информационной системы ООО «СЦСО Надежда» принял решение ориентироваться на требования, предъявляемые к государственным информационным системам, обрабатывающим сведения не составляющих государственную тайну. Данные требования прописаны в федеральном законе «О защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (в редакции приказа ФСТЭК России от 15 февраля 2017 г. N 27).

I. Общие положения

1. Настоящие Требования разработаны в соответствии с Федеральным законом от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3448; 2010, N 31, ст. 4196; 2011, N 15, ст. 2038; N 30, ст. 4600; 2012, N 31, ст. 4328), а также с учетом национальных стандартов Российской Федерации в области защиты информации и в области создания автоматизированных систем (далее – национальные стандарты).

2. В документе устанавливаются требования к обеспечению защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее – информация), от утечки по техническим каналам, несанкционированного доступа, специальных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения или блокирования доступа к ней (далее – защита информации) при обработке указанной информации в государственных информационных системах.

Настоящие Требования могут применяться для защиты общедоступной информации, содержащейся в государственных информационных системах, для достижения целей, указанных в пунктах 1 и 3 части 1 статьи 16 Федерального закона

от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации».

В документе не рассматриваются требования о защите информации, связанные с применением криптографических методов защиты информации и шифровальных (криптографических) средств защиты информации.

3. Настоящие Требования являются обязательными при обработке информации в государственных информационных системах, функционирующих на территории Российской Федерации, а также в муниципальных информационных системах, если иное не установлено законодательством Российской Федерации о местном самоуправлении.

Настоящие Требования не распространяются на государственные информационные системы Администрации Президента Российской Федерации, Совета Безопасности Российской Федерации, Федерального Собрания Российской Федерации, Правительства Российской Федерации, Конституционного Суда Российской Федерации, Верховного Суда Российской Федерации и Федеральной службы безопасности Российской Федерации.

4. Настоящие Требования предназначены для обладателей информации, заказчиков, заключивших государственный контракт на создание государственной информационной системы (далее – заказчики) и операторов государственных информационных систем (далее – операторы).

Лицо, обрабатывающее информацию, являющуюся государственным информационным ресурсом, по поручению обладателя информации (заказчика) или оператора и (или) предоставляющее им вычислительные ресурсы (мощности) для обработки информации на основании заключенного договора (далее – уполномоченное лицо), обеспечивает защиту информации в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации. В договоре должна быть предусмотрена обязанность уполномоченного лица обеспечивать защиту информации, являющейся государственным информационным ресурсом, в соответствии с настоящими Требованиями.

5. При обработке в государственной информационной системе информации, содержащей персональные данные, настоящие Требования применяются наряду с требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119 (Собрание законодательства Российской Федерации, 2012, N 45, ст. 6257).

6. По решению обладателя информации (заказчика) или оператора настоящие Требования могут применяться для защиты информации, содержащейся в негосударственных информационных системах.

7. Защита информации, содержащейся в государственной информационной системе (далее – информационная система), обеспечивается путем выполнения обладателем информации (заказчиком) и (или) оператором требований к организации защиты информации, содержащейся в информационной системе, и требований к мерам защиты информации, содержащейся в информационной системе [17].

Выводы по разделу один:

Были проанализированы СЗИ выделены основные плюсы и минусы. Сформировано решение об использовании: «Соболь 3.0», «SecretNetStudio 8.2», «Vipnet-client 4.3».

2 ОБНОВЛЕНИЕ СЗИ НА ПРЕДПРИЯТИИ ООО «СЦСО НАДЕЖДА»

2.1 Общий алгоритм построения защиты информации

Согласно владельцам информационной системы ООО «СЦСО Надежда» алгоритм построения защиты предприятия происходит согласно пунктам:

- Изучение существующей сети организации;
- Предъявление требований к корпоративной сети передачи данных (далее – КСПД) и выбор средств защиты информации для построения системы защиты субъектов предпринимательской деятельности (далее – СПД);
- Конфигурирования ЛВС с учетом требования безопасности;
- Ограничение доступа в режим BIOS с помощью парольной защиты;
- Монтаж и настройка СЗИ;
- Настройка межсетевого экрана.

2.2 Защита BIOS и загрузчика системы

Защита паролем BIOS (или аналога) и загрузчика системы может помешать неавторизованным пользователям, имеющим физический доступ к компьютеру, загрузить его со сменного носителя или стать пользователем root в монопольном режиме. Но меры безопасности, принимаемые для защиты от таких атак, должны зависеть от важности информации, хранящейся в ПК.

Есть две основные причины защиты паролем BIOS компьютера:

Предотвратить изменение настроек BIOS – если взломщик имеет доступ к BIOS, он может настроить загрузку с съемного носителя или компакт-диска. Это позволит ему войти в монопольный режим или режим восстановления, после чего он сможет внедрить в систему вредоносные программы или скопировать важные данные.

Предотвратить загрузку системы – в некоторых BIOS загрузку системы также можно защитить паролем. Если эта защита включена, взломщику нужно будет ввести пароль, прежде чем BIOS запустит загрузчик системы.

2.3 Инсталляция СЗИ «Соболь»

Инсталляция СЗИ Соболь производится согласно следующему алгоритму:

1. Установка платы расширения
2. Инициализация платы расширения
3. Настройка СЗИ Соболь

2.3.1 Для установки платы PCI-E необходимо действовать по следующей инструкции

Шаг 1. Выключить ПК;

Шаг 2. Открыть корпус системного блока и снять перемычку, установленную на разъем J0 платы Соболь 3.0;

Шаг 3. Установить плату.

Для использования механизма сторожевого таймера в режиме автоматической перезагрузки ПК необходимо:

– отключить штекер стандартного кабеля кнопки «Reset» от разъема «Reset», расположенного на материнской плате;

– подключить штекер стандартного кабеля кнопки «Reset» к разъему «RST» платы комплекса «Соболь» (Рисунок 2.1);

– подключить штекер кабеля механизма сторожевого таймера, входящего в комплект поставки, к разъему платы «WD»;

– подключить другой штекер данного кабеля к разъему «Reset», расположенному на материнской плате.

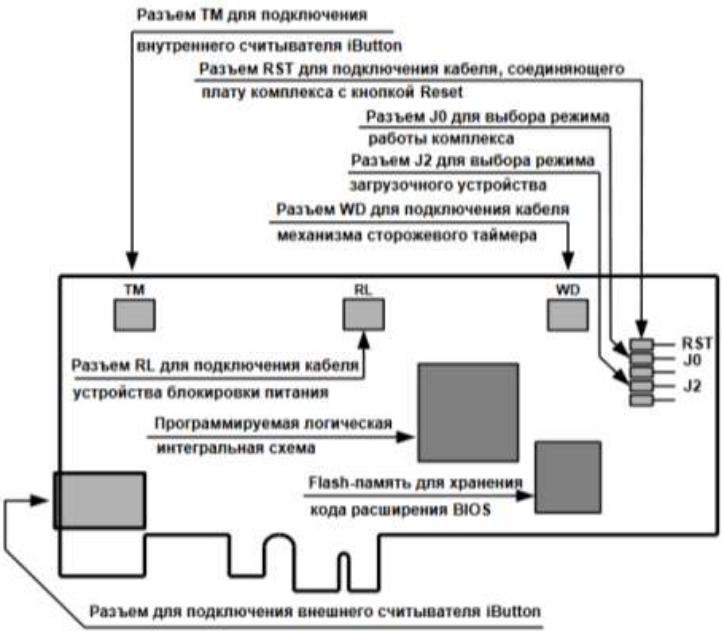


Рисунок 2.1 – Расположение разъемов на плате PCI-E

2.3.2 Инициализация комплекса СЗИ «Соболь»

Запуск процедуры инициализации осуществляется согласно следующему алгоритму действий:

1 шаг. Перед запуском ПАК Соболь 3.0 предварительно необходимо в BIOS определить плату первым загрузочным устройством;

2 шаг. Осуществляется перезагрузка ПК;

3 шаг. Далее управление передается ПАК «Соболь». На экране будет представлено окно которое можно наблюдать на рисунке 2.2.

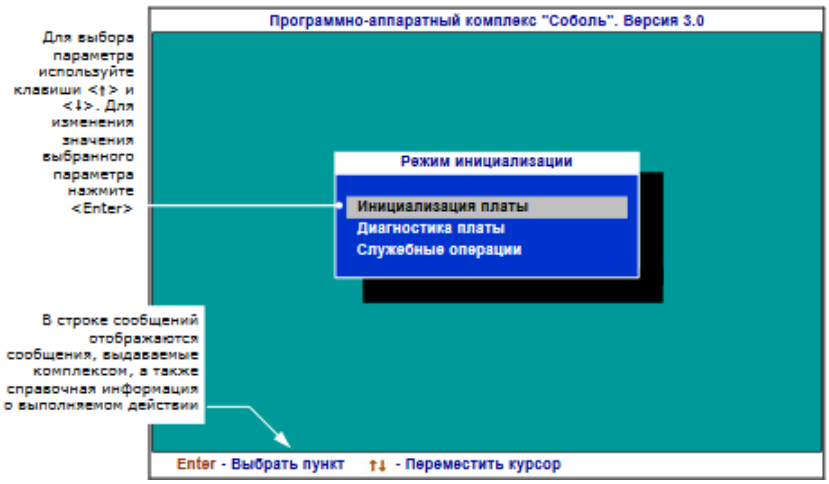


Рисунок 2.2 – Режим инициализации

Перед инициализацией комплекса также предоставляется возможность отформатировать персональный идентификатор iButton (микросхема, заключённая в стандартный круглый корпус из нержавеющей стали, диаметром 16.3 мм).

Примечание [ПW1]: Что это и для чего делается

2.3.3 Настройка общих параметров

Перечень настроек СЗИ соболь представлен следующим списком:

– Версия криптографической схемы обеспечивает совместимость с предыдущими версиями BIOS.

– Число попыток тестирования датчика случайных чисел (далее – ДСЧ). Определяет число попыток тестирования правильности работы ДСЧ комплекса, выполняемого при входе в систему. Параметр может принимать значения от 1 до 3. Тестирование ДСЧ выполняется до первой удачной попытки, после чего тестирование прекращается и считается завершившимся успешно. Работа комплекса продолжается. Если же число неудачных попыток тестирования ДСЧ достигло числа, заданного данным параметром, выдается сообщение об ошибке тестирования ДСЧ.

– Тестирование ДСЧ для пользователя. Позволяет включить или отключить тестирование правильности работы ДСЧ комплекса «Соболь», выполняющее-

ся при входе в систему пользователей. Тестирование ДСЧ при входе в систему администратора отключить нельзя, оно выполняется всегда. Параметр может принимать два значения: «Да» – тестирование ДСЧ выполняется, «Нет» – тестирование ДСЧ отключено.

– Показ статистики пользователя. Позволяет разрешить или запретить вывод на экран информационного окна, содержащего статистические сведения о работе пользователя. Окно появляется на экране после успешной идентификации пользователя. Параметр может принимать два значения: «Да» – разрешить вывод окна, «Нет» – запретить вывод окна.

– Минимальная длина пароля. Настройка СЗИ производится следующим образом. Определяется минимальная длина пароля пользователя в символах. Пользователю нельзя назначить пароль, число символов в котором меньше числа, заданного этим параметром. Параметр может принимать значения от 0 до 16. Если значение этого параметра равно «0», пользователю можно назначить пустой пароль, разрешив ему входить в систему без указания пароля (запрос пароля на экране не появится). Если при увеличении значения этого параметра длина паролей некоторых пользователей окажется меньше нового значения параметра, при входе в систему им будет предложено сменить свой старый пароль, без чего они не смогут загрузить ОС.

– Предельное число неудачных входов пользователя. Определяет, сколько раз пользователь может допустить ошибку при входе в систему, указав неверный пароль. Параметр может принимать значения от 0 до 65535. Значение «0» означает, что число неудачных попыток входа пользователей в систему не ограничено. Если число неудачных попыток входа пользователя в систему равно числу, заданному этим параметром, вход этого пользователя в систему будет автоматически блокирован. Если текущее число неудачных входов пользователя в систему меньше значения этого параметра и данный пользователь успешно вошел в систему, то значение счетчика неудачных попыток входа автоматически сбрасывается (приравнивается к нулю).

– Период тестирования сторожевого таймера. Определяет периодичность, с которой будет выполняться процедура тестирования механизма сторожевого таймера. Параметр может принимать значения от 0 до 999 дней. Значение «0» означает, что тестирование механизма сторожевого таймера не выполняется. Процедура тестирования механизма сторожевого таймера выполняется при входе пользователя в систему с периодичностью, заданной данным параметром.

– Поддержка USB – идентификаторов. Определяет типы используемых идентификаторов.

На экране монитора отображается следующий диалог (Рисунок 2.3).

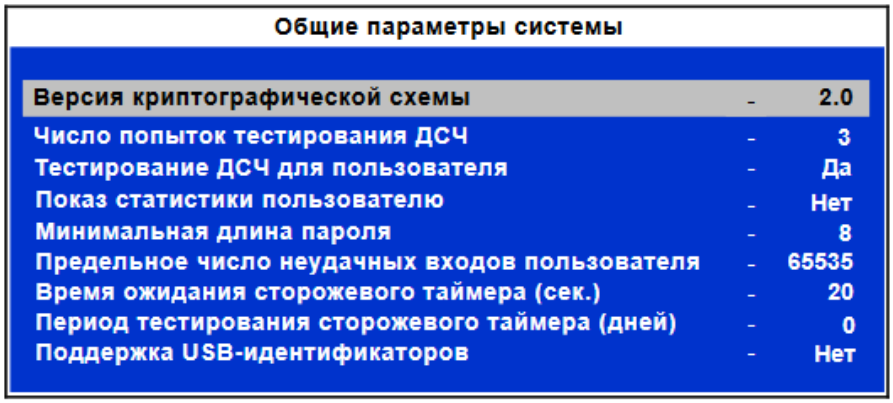


Рисунок 2.3 – Диалог настройки общих параметров

В данном диалоговом окне нас интересует параметр «Время ожидания сторожевого таймера», который определяет интервал времени в секундах, по истечении которого осуществляется автоматическая блокировка компьютера, при условии, что за это время управление не передано расширению BIOS комплекса «Соболь». Рекомендуемое время ожидания сторожевого таймера определяется автоматически на этапе инициализации комплекса. В дальнейшем администратор может корректировать значение параметра для платы PCI-E от 4 до 512 секунд с дискретностью 2 секунды (4, 6, 8, 10 и т.д).

В завершении настройки СЗИ необходимо зарегистрировать учетную запись администратора, которая позволит регистрировать учетные записи пользователей. При регистрации администратора ему назначается пароль и присваивается персональный идентификатор.

2.4 Установка и настройка межсетевого экрана

Согласно проведенному анализу ПО было принято решение использовать сертифицированный продукт Secret Net Studio 8.2.

2.4.1 Установка межсетевого экрана Secret Net Studio 8.2

Установка проводится согласно руководству пользователя версии Secret Net Studio 8.

2.4.2 Настройка межсетевого экрана Secret Net Studio 8.2

На рисунке представлен скриншот окна настройки «Межсетевого экрана» Secret Net Studio 8.2 (Рисунок 2.6).

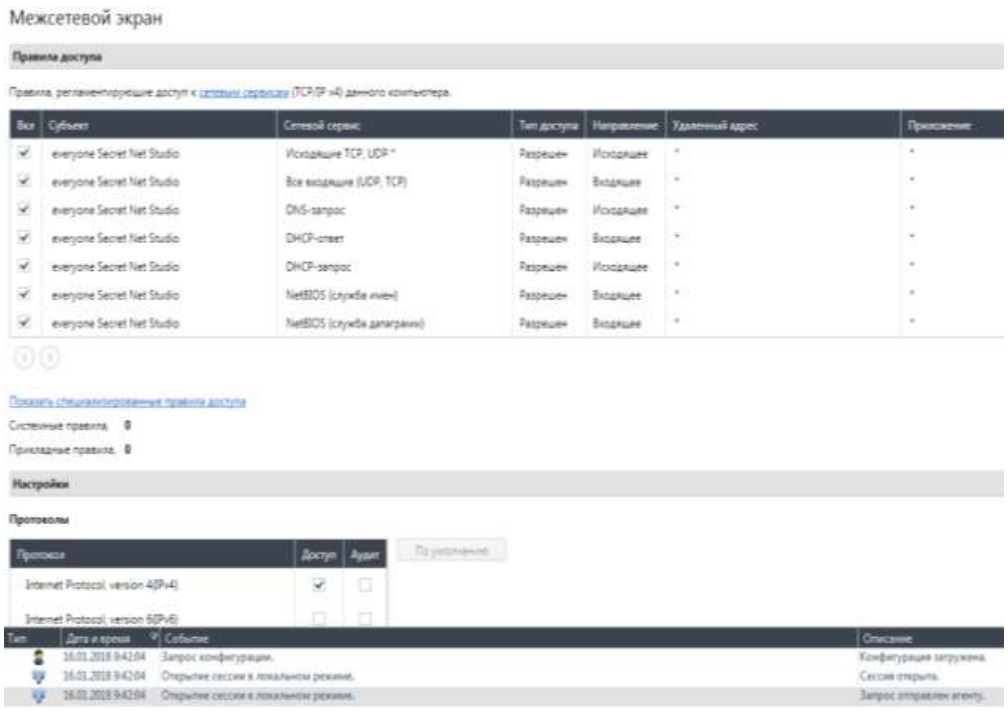


Рисунок 2.6 – Управление правилами доступа

В области настройки параметров межсетевого экрана перейти к разделу «Правила доступа».

Правила доступа

Правила, регламентирующие доступ к сетевым сервисам (TCP/IP v4) данного компьютера.

Вкл	Субъект	Сетевой сервис	Тип доступа	Направление
☑	everyone Secret Net Studio	Исходящие TCP, UDP *	Разрешен	Исходящее
☑	everyone Secret Net Studio	Все входящие (UDP, TCP)	Разрешен	Входящее
☑	everyone Secret Net Studio	DNS-запрос	Разрешен	Исходящее
☑	everyone Secret Net Studio	DHCP-ответ	Разрешен	Входящее
☑	everyone Secret Net Studio	DHCP-запрос	Разрешен	Исходящее
☑	everyone Secret Net Studio	NetBIOS (служба имен)	Разрешен	Входящее
☑	everyone Secret Net Studio	NetBIOS (служба датаграмм)	Разрешен	Входящее

Рисунок 2.7 – Правила доступа

2.4.3 Основные понятия протоколов управления межсетевого экрана

TCP (англ. Transfer Control Protocol) – протокол управления передачей. Он служит для обеспечения и установление надежного соединения между двумя устройствами и надежную передачу данных. При этом протокол TCP контролирует оптимальный размер передаваемого пакета данных, осуществляя новую посылку при сбое передачи [1].

IP (англ. Internet Protocol) – интернет протокол или адресный протокол – основа всей архитектуры передачи данных. Протокол IP служит для доставки сетевого пакета данных по нужному адресу. При этом информация разбивается на пакеты, которые независимо передвигаются по сети до нужного адресата.

DNS (англ. Domain Name System – система доменных имён) — распределённая система преобразования имени хоста (компьютера или другого сетевого устройства) в IP адрес.

DHCP (англ. Dynamic Host Configuration Protocol – протокол динамической настройки узла) – сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP.

NetBIOS (англ. Network Basic Input/Output System) – протокол для работы в локальных сетях на персональных ЭВМ типа IBM/PC, разработан в виде интерфейса, который не зависит от фирмы-производителя. [7]

Для каждого правила в таблице 2.4 отображены данные.

Таблица 2.4 – Значение правил

Столбец	Значение
Вкл	Управление работой правила: – Отметка отсутствует – работа правила временно приостановлена; – Отметка установлена – правило включено;
Субъект	Имя учетной записи или группы учетных записей, для которых действует правило

Продолжение таблицы 2.4

Столбец	Значение
Сетевой сервис	Наименование сетевого сервиса, для которого действует правило
Тип доступа	Тип доступа к защищаемому компьютеру: – «Разрешен» – «Запрещен»
Направление	Направление трафика, для которого действует правило
Удаленный адрес	Имя или IP-адрес компьютера, для которого действует правило. Символ * (звездочка) означает, что правило действует для всех удаленных компьютеров
Приложение	Путь к приложению, для которого действует правило

Порядок обработки пакетов в Secret Net Studio зависит от направления сетевого трафика:

– Входящие пакеты – первоначально производится проверка на соответствие настройкам сетевых протоколов, затем – на соответствие системным правилам, а затем, если пакет пропущен, – на соответствие правилам доступа;

– Исходящие пакеты – сначала производится проверка на соответствие правилам доступа, затем – на соответствие системным правилам, а затем, если пакет пропущен, – на соответствие настройкам сетевых протоколов.

По умолчанию правила доступа к объектам обрабатываются в порядке их создания и расположения в таблице правил. Наивысшим приоритетом обладают правила, расположенные в начальных строках таблицы.

2.5 Инсталляция и настройка защищённого канала

Для решения вопроса о безопасности соединения было принято решение использовать ПО ViPNet Client по причине создания своей виртуальной сети.

ViPNet Client – ПО для защиты трафика на рабочих местах пользователей. ViPNet Client фильтрует весь входящий и исходящий трафик ПК и позволяет обмениваться данными с другими узлами ViPNet по защищенному VPN-каналу.

Перед установкой ViPNet Client стоит убедиться, в том что на ПК правильно заданы системное время и региональные настройки. ViPNet Client может быть несовместим с антивирусами, которые имеют функцию сетевого экрана.

Для работы ViPNet Client требуется ключ ViPNet. Для того, чтобы установить ключ необходимо запустить файл с расширением «.dst» сгенерированный с помощью с помощью Vipnet Administrator.

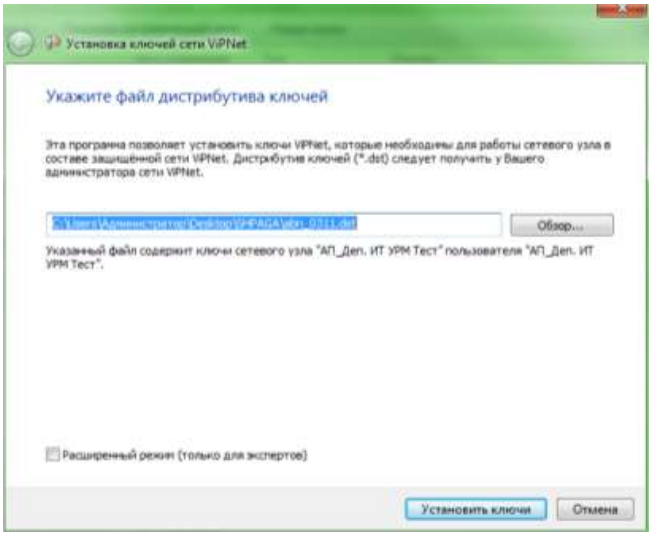


Рисунок 2.8 – Установка ключа

В дальнейшем программа ViPNet Client будет запускаться автоматически. Аутентификацию в ViPNet Client необходимо выполнить перед входом в операционную систему. Для входа в программу вводим пароль либо подключаем устройство аутентификации и вводим ПИН-код. После откроется окно программы ViPNet Монитор.

Рисунок 2.9 – Запуск программы

2.5.1 Работа в защищенной сети

Список узлов ViPNet, с которыми можем обмениваться данными по защищенному VPN-каналу, отображается в программе ViPNet Монитор в разделе «Защищенная сеть». Чтобы использовать возможности работы в защищенной сети, необходимо выбрать нужный узел.

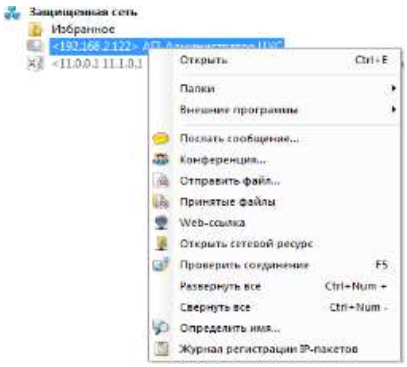


Рисунок 2.10 – Защищенная сеть

2.5.2 Настройка сетевых фильтров

Сетевые фильтры используются, чтобы пропускать или блокировать трафик по определенным признакам. Сетевые фильтры, настроенные по умолчанию, блокируют входящий открытый (незашифрованный) трафик за исключением протоколов DHCP, NetBIOS, WINS. При необходимости вы можете настроить собственные сетевые фильтры для открытого и зашифрованного трафика.

Фильтры открытой сети

Вкл.	Действие	Имя	Источник	Назначение	Протокол	Расписание
Настраиваемые фильтры						
☑	Разрешить	Фильтр 1	Все	Все	Все	Все
☑	Разрешить	DHCP-трафик	Все	Все	DHCP	Все
☑	Разрешить	NetBIOS- и WINS-трафик	Все	Все	NetBIOS-DGM	Все
☑	Разрешить	IGMP-трафик	Все	Все	IGMP	Все
☑	Разрешить	PING	Все	Все	PING	Все
☑	Разрешить	Исходящий трафик	Мой узел	Все	Все	Все
Фильтры по умолчанию						
☑	Блокировать	Прочий трафик	Все	Все	Все	Все

Рисунок 2.11 – Фильтры открытой сети

2.5.3 Контроль приложений

Программа ViPNet Контроль приложений обеспечивает контроль над сетевой активностью приложений, установленных на компьютере. Если какая-либо программа пытается получить доступ к сети, на экране появляется предупреждение. В окне предупреждения необходимо выбрать, разрешить программе доступ к сети или запретить.

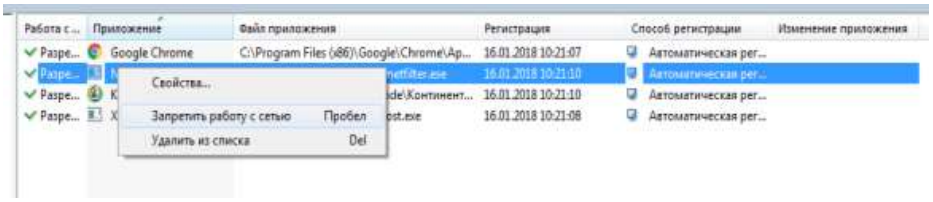


Рисунок 2.12 – Контроль приложения Windows

Чтобы просмотреть список приложений, которым разрешен или запрещен доступ к сети, в программе ViPNet Монитор в меню Приложения выберем пункт «Контроль приложений». При необходимости добавляем приложения в список или изменяем разрешения для добавленных ранее приложений.

Выводы по разделу два:

В данном разделе рассмотрены предпринятые меры по защите КСПД, которые внедрены на предприятии ООО «СЦСО Надежда», а именно внедрены СЗИ: «Соболь 3.0», «SecretNetStudio 8.2», «Vipnet-client 4.3».

Внедренные СЗИ позволили обеспечить защиту от несанкционированного доступа к персональным данным предприятия согласно требований ФСТЭК.

3 ОРГАНИЗАЦИОННО-ЭКОНОМИЧЕСКИЙ РАЗДЕЛ

В выпускной квалификационной работе ставится цель – сконфигурировать и защитить корпоративную сеть организации от несанкционированного доступа на базе сертифицированных программно-аппаратных продуктов удовлетворяющих требованием регуляторов ФСТЭК и ФСБ в области защите информации [17].

Ввиду большой сложности проведения работ по созданию программно-аппаратного комплекса средств защиты информации, применялись системы сетевого планирования и управления. Такие системы основываются на применении сетевых моделей планируемых процессов, допускающих использование современной вычислительной техники.

Основной частью показателей экономической эффективности является расчет сметы затрат на разработку программного комплекса средств защиты информации включающую в себя:

1) затраты на трудовые ресурсы (заработная плата исполнителей);
2) отчисления с заработной платы;
3) затраты на оборудование;
4) затраты на расходные материалы;
5) прочие расходы.

3.1 Сетевой метод организации работ

Состав и содержание работ по внедрению программно-аппаратного комплекса СЗИ представлен в таблице 3.1.

Таблица 3.1 – Состав и содержание работ

№ пункта	Содержание работ	Начало	Окончание	Длительность	Исполнители
Стадия 1. Техническое задание					
1	Постановка задачи	0	1	1	Инженер
2	Сбор исходных информационных материалов	1	2	1	Инженер
3	Обоснование необходимости внедрения программно-аппаратного комплекса СЗИ	1	2	1	Инженер
4	Определение требований к техническим средствам	4	5	1	Инженер
5	Обоснование принципиальной возможности решения поставленной задачи	3	4	1	Инженер
6	Согласование и утверждение внедрения программно-аппаратного комплекса СЗИ	5	6	1	Инженер
Стадия 2. Эскизный проект					
7	Уточнение методов решения задачи	6	7	1	Инженер
8	Анализ существующих СЗИ	7	8	1	Инженер
Стадия 3. Технический проект					
9	Изучение существующей сети организации	7	8	1	Инженер

Продолжение таблицы 3.1

№ пункта	Содержание работ	Начало	Окончание	Длительность	Исполнители
10	Предъявление требований к КСПД и выбор средств защиты информации для построения системы защиты СПД	8	9	1	Инженер
11	Разработка плана мероприятий по внедрению программно-аппаратного комплекса СЗИ	9	10	1	Инженер
12	Разработка пояснительной записки к ТП	9	11	2	Инженер
13	Согласование и утверждение ТП	11	12	1	Инженер
Стадия 4. Рабочий проект					
14	Установка и настройка ПАК Соболь	11	19	8	Инженер
15	Установка программных средств защиты информации (СЗИ)	13	16	3	Инженер
16	Разработка эксплуатационных документов	16	17	1	Инженер
17	Согласование и утверждение порядка и методики тестирования	17	18	1	Инженер
18	Тестирование функциональных возможностей СЗИ	17	18	1	Инженер
19	Корректировка СЗИ и документации по результатам тестирования	17	18	1	Инженер
Стадия 5. Внедрение					
20	Подготовка и установка программно-аппаратного комплекса, передача документации	19	20	1	Инженер
21	Обучение персонала	20	21	1	Инженер
22	Ввод в эксплуатацию	21	22	1	Инженер

Количество событий – 22.

Количество работ – 22.

Количество дней на разработку – 22.

3.2 Состав участников в пуско-наладке СЗИ

В пуско-наладке программно-аппаратного комплекса СЗИ задействован один инженер (таблица 3.2).

Таблица 3.2 – Разработчики

Код	Должность	Оклад. в месяц, руб.	Срок работы, дн.
И	инженер	45000	22

СЗИ, используемое для реализации данного комплекса представлено в таблице 3.3.

Таблица 3.3 – Программно-аппаратный комплекс СЗИ

Название	Характеристики, марка	Кол-во	Цена единицы, руб.	Общая стоимость, руб.
ПАК Соболь 3.0	PCI express	9	12 500	112 500
Программное обеспечение Secret Net Studio 8.2	Постоянная + Дополнительная защита (три года)	9	16 055	144 495
Vipnet 4.3	Передача права на использование ПО ViPNet Client for Windows 4.x (КС2)	9	7 790	70 110
Итого				327 105

3.2.1 Расчет заработной платы инженера

Расчет основной заработной платы выполняется на основе трудоемкости выполнения каждого этапа в человеко-днях и величины месячного должностного оклада исполнителя. Среднее количество рабочих дней в месяце равно 22. Следовательно, дневная заработная плата определяется делением размера ежемесячной заработной платы на количество рабочих дней в месяце. Произведение трудоемко-

сти на сумму дневной заработной платы определяет затраты по зарплате для каждого работника на все время разработки.

Расчета заработной платы разработчиков рассчитывается по формуле 1:

$$З_i = Ok \cdot N, \quad (1)$$

где Ok – оклад разработчика (руб.);

N – кол-во дней (см. таблицу 3.1).

Отчисления с заработной платы включают в себя:

1) отчисления в Пенсионный фонд Российской Федерации (по состоянию на 2018 год составляют 22%);

2) отчисления в Фонд социального страхования Российской Федерации (по состоянию на 2018 год составляет 2,9%);

3) Федеральный фонд обязательного медицинского страхования и территориальные фонды обязательного медицинского страхования (по состоянию на 2017 год составляет 5,1%).

Итоговая сумма отчислений с заработной платы специалиста составляет:

(22% + 2,9% + 5,1%) * 45000= 13500 руб.

Таблица 3.4 – Заработная плата

Разработчик	Инженер	Всего
Зарплата, руб. в месяц	45000	45000
Отчисления во внебюджетные фонды (30%)	13500	13500
Итого	58500	

3.2.2 Расчет стоимости амортизации оборудования и программного обеспечения

Амортизация оборудования – это исчисленный в денежном выражении износ основных средств в процессе их применения, производственного использова-

ния. Амортизация есть одновременно средство, способ, процесс перенесения стоимости изношенных средств труда на произведенный с их помощью продукт.

Стоимость комплекса средств защиты (ПАК Соболь, Secret Net Studio 8.2, Vipnet 4.3) составила 327 105 тысяч рублей.

Формула для расчета стоимости амортизации (аренды) оборудования:

Норма амортизации оборудования равна 14,1%. Рассчитываем стоимость аренды оборудования по формуле 2:

$$Ца_j = \frac{C_j \cdot A}{N}, \qquad (2)$$

где $Ца_j$ – стоимость j-го вида оборудования;

C_j – цена оборудования;

A – годовая амортизация оборудования (14,1%);

N – кол-во рабочих дней в году (265).

$$Ца_j = \frac{327105 \bullet 0.141 \bullet 22}{265} = 3828.98$$

Таблица 3.5 – Амортизация оборудования

Комплекс СЗИ	1	Итог
Дни работ	22	22
Стоимость амортизации, руб.	3828,98	3828,98

3.2.3 Расчет затрат по потреблению электроэнергии

По статистическим данным, компьютер потребляет 800 Вт/ч. На рассмотренном предприятии используется 9 ПК, которые в общей сложности потребляют 4,5 кВт/ч. Используем эти данные для расчета затрат на электроэнергию.

Расчет затрат на электроэнергию Z, руб., ведется по формуле 3:

$$Z = W \cdot Tp \cdot t \cdot n, \qquad (3)$$

где W – потребляемая мощность кВт/день;

t – тарифная ставка, руб.;

Tp – количество рабочих часов, 4;

n – количество рабочих дней, день 22.

Тарифная ставка по ХМАО равна 2,68 руб./ч.

Z=4,5•4•2,68•22=1061,28 рублей

3.2.4 Контрагентские расходы

«Контрагентские расходы» включается стоимость работ, выполненных сторонними организациями и предприятиями по заказу организации. В нашем случае такими расходами являются использование интернета. В таблице 3.6 представлен расчет затрат по статье «Контрагентские расходы».

Таблица 3.6 – Контрагентские расходы

Наименование работы	Кол-во	Цена за единицу, руб.	Стоимость, руб.
Предоставление доступа в Интернет	1 месяца (безлимит)	800	800
Итого:			800

3.2.5 Накладные расходы

Накладные расходы составляют десять процентов от всех насчитанных на проведение работы расходов, а именно – 4798,026 рублей.

10%•(45000+13500+3828,98+1061,28+250) = 4798,026 рублей.

3.2.6 Себестоимость программно-аппаратного продукта

Расчет себестоимости программно-аппаратного комплекса является суммой всех расходов для разработки, представленной в таблице 3.8.

Таблица 3.8 – Общая смета затрат

Наименование расходов	Содержание	Порядок расчета	Затраты, руб.
Амортизация	Амортизации оборудования	14,1% годовых от стоимости	1061,28
Электроэнергия	Затраты на электроэнергию	Расчет из см. п. 4.2.4	3828,98
Контрагентские расходы	Затраты на интернет	Тарифная ставка провайдера	800
Заработная плата	Зарплата инженеров	Расчет из см. п. 4.2.2	45000
Налог	Отчисления в государственные фонды	30% от суммы заработной платы	13500
Расходы	Накладные расходы	10% от общей суммы затрат	6538,026
Итого			70 728,52

В случае данной работы стоимость программы равна отпускной цене программы, то есть не включает в себя прибыль, так как разработка ведется штатными специалистами конечная стоимость программно-аппаратного комплекса СЗИ будет равна 70 728,52рублей.

3.3 Оценка технико-экономической эффективности

Важным фактором, влияющим на процесс формирования цены программного продукта, является конкуренция на рынке, которую необходимо учитывать. Необходимость разработки данного программного продукта очевидна, поскольку – аналоги не отвечают требованием ФСТЭК и ФСБ и не обеспечивают необходимые функциональные требования для предприятия либо имеют высокую стоимость за счет установки дополнительного оборудования.

Среднерыночная стоимость оборудования для предприятия системой приведена в таблице 3.9.

Таблица 3.9 – Коммерческое предложение от сторонней организаций

Статья расходов	Стоимость	Количество	Общая стоимость, руб.
Программно-аппаратного комплекса	45000	9	405000
Установка программного продукта	15000	9	135000
Итого	4000		

Таблица 3.10 – Стоимость разработанного программно-аппаратного комплекса СЗИ

Статья расходов	Стоимость	Количество	Общая стоимость, руб.
Программно-аппаратного комплекса	36345	9	327105
Итого	327105		

С учетом себестоимости разработанного программного комплекса СЗИ экономия на внедрение составит 77 105 рублей, что позволит исключить расходы, связанные с внедрением СЗИ.

Выводы по разделу три:

Важным фактором, влияющим на процесс формирования цены программного продукта, является конкуренция на рынке, которую необходимо учитывать. В данном разделе произведены расчеты, которые доказывают экономическую эффективность и конкурентоспособность разработанного программного-аппаратного комплекса СЗИ.

4 БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

С развитием научно-технического прогресса немаловажную роль играет возможность безопасного исполнения людьми своих трудовых обязанностей. В связи с этим была создана и развивается наука о безопасности труда и жизнедеятельности человека.

Цель и содержание безопасность жизнедеятельности:

1) обнаружение и изучение факторов окружающей среды, отрицательно влияющих на здоровье человека;

2) ослабление действия этих факторов до безопасных пределов или исключение их, если это возможно;

На рабочем месте должны быть предусмотрены меры защиты от возможного воздействия опасных и вредных факторов производства. Уровни этих факторов не должны превышать предельных значений, оговоренных правовыми, техническими и санитарно-техническими нормами. Эти нормативные документы обязывают к созданию на рабочем месте условий труда, при которых влияние опасных и вредных факторов на работающих либо устранено совсем, либо находится в допустимых пределах.

Данный раздел ВКР посвящен рассмотрению следующих вопросов:

1) определение оптимальных условий труда инженера-программиста;

2) требования к производственным помещениям (освещение, микроклимат, шум и вибрация, электромагнитное и ионизирующее излучение);

3) эргономические требования к рабочему месту;

4) режим труда;

5) требования к электробезопасности;

6) организация пожарной профилактики;

4.1 Характеристика условий труда инженера

Научно-технический прогресс внес серьезные изменения в условия производственной деятельности работников умственного труда. Их труд стал более интенсивным, напряженным, требующим значительных затрат умственной, эмоциональной и физической энергии. Это потребовало комплексного решения проблем эргономики, гигиены и организации труда, регламентации режимов труда и отдыха.

В настоящее время компьютерная техника широко применяется во всех областях деятельности человека. При работе с компьютером человек подвергается воздействию ряда опасных и вредных производственных факторов: электромагнитных полей (диапазон радиочастот: ВЧ, УВЧ и СВЧ), инфракрасного и ионизирующего излучений, шума и вибрации, статического электричества и др.

Работа с компьютером характеризуется значительным умственным напряжением и нервно-эмоциональной нагрузкой операторов, высокой напряженностью зрительной работы и достаточно большой нагрузкой на мышцы рук при работе с клавиатурой ЭВМ. Большое значение имеет рациональная конструкция и расположение элементов рабочего места, что важно для поддержания оптимальной рабочей позы человека-оператора.

В процессе работы с компьютером необходимо соблюдать правильный режим труда и отдыха. В противном случае у персонала отмечаются значительное напряжение зрительного аппарата с появлением жалоб на неудовлетворенность работой, головные боли, раздражительность, нарушение сна, усталость и болезненные ощущения в глазах, в пояснице, в области шеи и руках.

4.2 Требования к производственным помещениям

4.2.1 Освещение

Правильно спроектированное и выполненное производственное освещение улучшает условия зрительной работы, снижает утомляемость, способствует повышению производительности труда, благотворно влияет на производственную среду, оказывая положительное психологическое воздействие на работающего, повышает безопасность труда и снижает травматизм.

Существует три вида освещения – естественное, искусственное и совмещенное (естественное и искусственное вместе). В помещениях вычислительных центров необходимо применение системы комбинированного освещения.

При выполнении работ категории высокой зрительной точности (наименьший размер объекта различения 0,3…0,5мм) величина коэффициента естественного освещения (далее – КЕО) должна быть не ниже 1,5%, а при зрительной работе средней точности (наименьший размер объекта различения 0,5…1,0 мм) КЕО должен быть не ниже 1,0%. В качестве источников искусственного освещения обычно используются люминесцентные лампы типа ЛБ или ДРЛ, которые попарно объединяются в светильники, которые должны располагаться над рабочими поверхностями равномерно

Требования к освещенности в помещениях, где установлены компьютеры, согласно СанПиН 2.2.2/2.4.1340-03 следующие: при выполнении зрительных работ высокой точности общая освещенность должна составлять 300лк, а комбинированная – 750лк; аналогичные требования при выполнении работ средней точности 300лк соответственно [13].

Кроме того, все поле зрения должно быть освещено достаточно равномерно – это основное гигиеническое требование. Иными словами, степень освещения помещения и яркость экрана компьютера должны быть примерно одинаковыми, т.к. яркий свет в районе периферийного зрения значительно увеличивает напряженность глаз и, как следствие, приводит к их быстрой утомляемости.

Для обеспечения нормируемых значений освещенности в помещениях следует не реже двух раз в год чистить стекла, оконные рамы и светильники и своевременно заменять перегоревшие лампы.

Рабочие места должны располагаться таким образом, чтобы естественный свет падал сбоку, преимущественно слева.

Оконные проемы должны быть оборудованы регулируемыми жалюзи, занавесями, внешними козырьками и др.

4.2.2 Параметры микроклимата

На рабочем месте, оснащенном монитором или ПК, а также в помещении должны выполняться требования к микроклимату.

Должна поддерживаться подходящая влажность воздуха, для чего могут быть применены специальные увлажнители воздуха или кондиционеры.

Допустимые и оптимальные параметры относительной влажности воздуха и температуры приведены в таблице 4.1.

Таблица 4.1 – Допустимые и оптимальные параметры влажности и температуры воздуха

Оптимальные параметры		Допустимые параметры	
Температура, С°	Относительная влажность, %	Температура, С°	Относительная влажность, %
19	62	18	39
20	58	22	31
21	55	-	-

Воздух в помещении должен соответствовать нормам по содержанию вредных химических веществ, а также аэронов. Уровень ионизации воздуха согласно СанПиН 2.2.2/2.4.1340-03 представлен в таблице 4.2 [14].

Таблица 4.2 – Уровни ионизации воздуха в помещениях

	Число ионов в 1см³ воздуха	
	N+	n–
Минимально необходимые	400	600
Оптимальные	1500 – 3000	300 – 5000
Максимально допустимые	50000	50000

Установленный в изученном помещении кондиционер установлен на поддержание оптимальной температуры и влажности.

Объем помещений, в которых размещены работники вычислительных центров, не должен быть меньше 19,5 $м^3$/человека с учетом максимального числа одновременно работающих в смену.

Для обеспечения комфортных условий используются как организационные методы (рациональная организация проведения работ в зависимости от времени года и суток, чередование труда и отдыха), так и технические средства (вентиляция, кондиционирование воздуха, отопительная система).

4.2.3 Шум и вибрация

Шум ухудшает условия труда оказывая вредное действие на организм человека. Работающие в условиях длительного шумового воздействия испытывают раздражительность, головные боли, головокружение, снижение памяти, повышенную утомляемость, понижение аппетита, боли в ушах и т. д. Такие нарушения в работе ряда органов и систем организма человека могут вызвать негативные изменения в эмоциональном состоянии человека вплоть до стрессовых. Под воздействием шума снижается концентрация внимания, нарушаются физиологические функции, появляется усталость в связи с повышенными энергетическими затратами и нервно-

психическим напряжением, ухудшается речевая коммутация. Все это снижает работоспособность человека и его производительность, качество и безопасность труда. Длительное воздействие интенсивного шума (выше 80 дБ) на слух человека приводит к его частичной или полной потере.

В таблице 4.3 указаны предельные уровни звука в зависимости от категории тяжести и напряженности труда, являющиеся безопасными в отношении сохранения здоровья и работоспособности.

Таблица 4.3 – Предельные уровни звука, дБ, на рабочих местах

Категория напряженности труда	Категория тяжести труда			
	I. Легкая	II. Средняя	III. Тяжелая	IV. Очен тяжелая
I. Мало напряженный	80	80	75	75
II. Умеренно напряженный	70	70	65	65
III. Напряженный	60	60	-	-
IV. Очень напряженный	50	50	-	-

Уровень шума на рабочем месте инженеров и операторов видеоматериалов не должен превышать 50дБА, а в залах обработки информации на вычислительных машинах – 65дБА. Для снижения уровня шума стены и потолок помещений, где установлены компьютеры, могут быть облицованы звукопоглощающими материалами. Уровень вибрации в помещениях вычислительных центров может быть снижен путем установки оборудования на специальные виброизоляторы.

4.2.4 Электромагнитное и ионизирующее излучения

Большинство ученых считают, что как кратковременное, так и длительное воздействие всех видов излучения от экрана монитора не опасно для здоровья персонала, обслуживающего компьютеры. Однако исчерпывающих данных относительно опасности воздействия излучения от мониторов на работающих с компьютерами не существует и исследования в этом направлении продолжаются.

Допустимые значения параметров неионизирующих электромагнитных излучений от монитора компьютера представлены в таблице 4.4.

Максимальный уровень рентгеновского излучения на рабочем месте оператора компьютера обычно не превышает 10мкбэр/ч, а интенсивность ультрафиолетового и инфракрасного излучений от экрана монитора лежит в пределах 10…100мВт/м^2.

Таблица 4.4 – Допустимые значения параметров неионизирующих электромагнитных излучений (в соответствии с СанПиН 2.2.2/2.4.1340-03) [14]

Наименование параметра	Допустимые значения
Напряженность электрической составляющей электромагнитного поля на расстоянии 50см от поверхности видеомонитора	10В/м
Напряженность магнитной составляющей электромагнитного поля на расстоянии 50см от поверхности видеомонитора	0,3А/м
Напряженность электростатического поля не должна превышать: для взрослых пользователей для детей дошкольных учреждений и учащихся средних специальных и высших учебных заведений	 20кВ/м 15кВ/м

Для снижения воздействия этих видов излучения рекомендуется применять мониторы с пониженным уровнем излучения (MPR-II, TCO-92, TCO-99), соблюдать регламентированные режимы труда и отдыха.

4.2.5 Эргономические требования к рабочему месту

Проектирование рабочих мест, снабженных видеотерминалами, относится к числу важных проблем эргономического проектирования в области вычислительной техники.

Рабочее место и взаимное расположение всех его элементов должно соответствовать антропометрическим, физическим и психологическим требованиям. Большое значение имеет также характер работы. В частности, при организации рабочего места программиста должны быть соблюдены следующие основные усло-

вия: оптимальное размещение оборудования, входящего в состав рабочего места и достаточное рабочее пространство, позволяющее осуществлять все необходимые движения и перемещения.

Эргономическими аспектами проектирования видеотерминальных рабочих мест, в частности, являются: высота рабочей поверхности, размеры пространства для ног, требования к расположению документов на рабочем месте (наличие и размеры подставки для документов, возможность различного размещения документов, расстояние от глаз пользователя до экрана, документа, клавиатуры и т.д.), характеристики рабочего кресла, требования к поверхности рабочего стола, регулируемость элементов рабочего места.

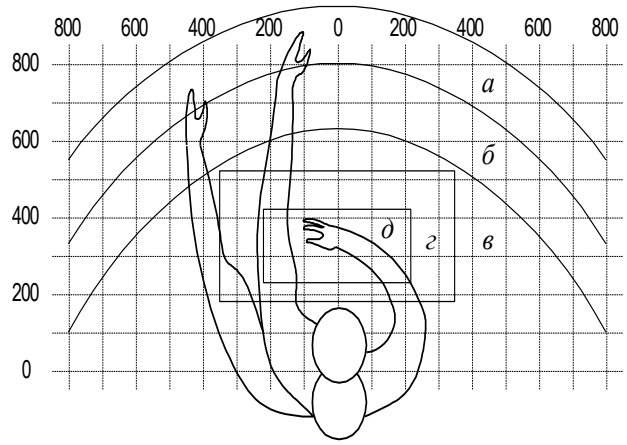
Главными элементами рабочего места программиста являются стол и кресло. Основным рабочим положением является положение сидя.

Рабочая поза сидя вызывает минимальное утомление программиста. Рациональная планировка рабочего места предусматривает четкий порядок и постоянство размещения предметов, средств труда и документации. То, что требуется для выполнения работ чаще, расположено в зоне легкой досягаемости рабочего пространства.

Моторное поле – пространство рабочего места, в котором могут осуществляться двигательные действия человека.

Максимальная зона досягаемости рук – это часть моторного поля рабочего места, ограниченного дугами, описываемыми максимально вытянутыми руками при движении их в плечевом суставе.

Оптимальная зона – часть моторного поля рабочего места, ограниченного дугами, описываемыми предплечьями при движении в локтевых суставах с опорой в точке локтя и с относительно неподвижным плечом.



а - зона максимальной досягаемости;
б - зона досягаемости пальцев при вытянутой руке;
в - зона легкой досягаемости ладони;
г - оптимальное пространство для грубой ручной работы;
д - оптимальное пространство для тонкой ручной работы.

Рисунок 4.1 – Зоны досягаемости рук в горизонтальной плоскости

Оптимальное размещение предметов труда и документации в зонах досягаемости (см. Рисунок 4.1):

ДИСПЛЕЙ – размещается в центре зоны «а»; (см. Рисунок 4.1)

СИСТЕМНЫЙ БЛОК – размещается в предусмотренной нише стола; (см. Рисунок 4.1)

КЛАВИАТУРА – в зоне «г/д»; (см. Рисунок 4.1)

МЫШЬ – в зоне «в» справа; (см. Рисунок 4.1)

СКАНЕР – слева в зоне «а/б»; (см. Рисунок 4.1)

ПРИНТЕР– находится справа, в зоне «а»; (см. Рисунок 4.1)

ДОКУМЕНТАЦИЯ – необходимая при работе в зоне легкой досягаемости ладони «в», а в выдвижных ящиках стола литература, неиспользуемая постоянно. (см. Рисунок 4.1)

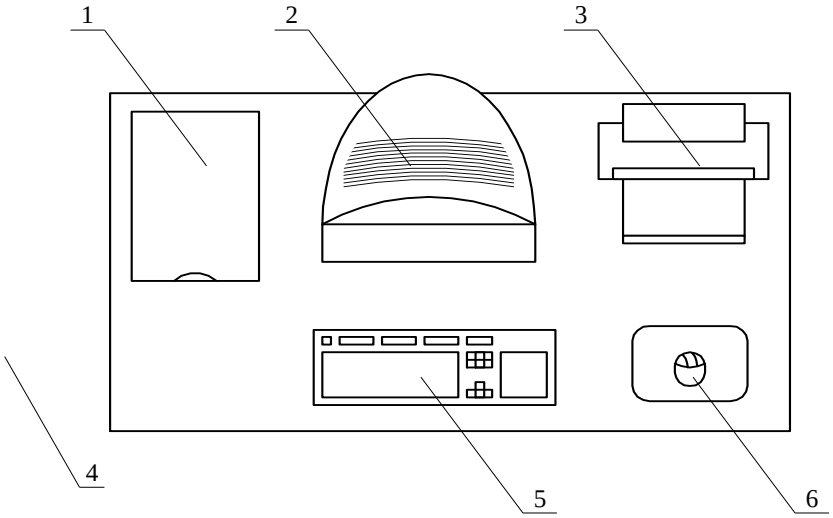


Рисунок 4.2 – Размещение основных и периферийных устройств

На рисунке 4.2 показан пример размещения основных и периферийных устройств, составляющих ПК на рабочем столе инженера.

1 – сканер, 2 – монитор, 3 – принтер, 4 – поверхность рабочего стола, 5 – клавиатура, 6 – манипулятор типа «мышь».

Для комфортной работы стол должен удовлетворять следующим условиям:

1) высота стола должна быть выбрана с учетом возможности сидеть свободно, в удобной позе, при необходимости опираясь на подлокотники;

2) нижняя часть стола должна быть сконструирована так, чтобы программист мог удобно сидеть, не был вынужден поджимать ноги;

3) поверхность стола должна обладать свойствами, исключающими появление бликов в поле зрения программиста;

4) конструкция стола должна предусматривать наличие выдвижных ящиков (не менее 3 для хранения документации, листингов, канцелярских принадлежностей).

5) высота рабочей поверхности рекомендуется в пределах 680-760 мм. Высота поверхности, на которую устанавливается клавиатура, должна быть около 650 мм.

Большое значение придается характеристикам рабочего кресла. Так, рекомендуемая высота сиденья над уровнем пола находится в пределах 420-550 мм. Поверхность сиденья мягкая, передний край закругленный, а угол наклона спинки – регулируемый.

Необходимо предусматривать при проектировании возможность различного размещения документов: сбоку от видеотерминала, между монитором и клавиатурой и т.п. Кроме того, в случаях, когда видеотерминал имеет низкое качество изображения, например заметны мелькания, расстояние от глаз до экрана делают больше (около 700 мм), чем расстояние от глаза до документа (300-450 мм). Вообще при высоком качестве изображения на видеотерминале расстояние от глаз пользователя до экрана, документа и клавиатуры может быть равным.

Положение экрана определяется:

1) расстоянием считывания (0,6…0,7м);

2) углом считывания, направлением взгляда на 20° ниже горизонтали к центру экрана, причем экран перпендикулярен этому направлению.

Должна также предусматриваться возможность регулирования экрана:

1) по высоте +3 см;

2) по наклону от -10° до +20° относительно вертикали;

3) в левом и правом направлениях.

Большое значение также придается правильной рабочей позе пользователя. При неудобной рабочей позе могут появиться боли в мышцах, суставах и сухожилиях. Требования к рабочей позе пользователя видеотерминала следующие:

1) голова не должна быть наклонена более чем на 20°,

2) плечи должны быть расслаблены,

3) локти под углом 80°…100°,

4) предплечья и кисти рук в горизонтальном положении.

Причина неправильной позы пользователей обусловлена следующими факторами: нет хорошей подставки для документов, клавиатура находится слишком высоко, а документы низко, некуда положить руки и кисти, недостаточно пространство для ног.

В целях преодоления указанных недостатков даются общие рекомендации: лучше передвижная клавиатура; должны быть предусмотрены специальные приспособления для регулирования высоты стола, клавиатуры и экрана, а также подставка для рук.

Существенное значение для производительной и качественной работы на компьютере имеют размеры знаков, плотность их размещения, контраст и соотношение яркостей символов и фона экрана. Если расстояние от глаз оператора до экрана дисплея составляет 60…80 см, то высота знака должна быть не менее 3мм, оптимальное соотношение ширины и высоты знака составляет 3:4, а расстояние между знаками – 15…20% их высоты. Соотношение яркости фона экрана и символов от 1:2 до 1:15.

Во время пользования компьютером медики советуют устанавливать монитор на расстоянии 50-60 см от глаз. Специалисты также считают, что верхняя часть видеодисплея должна быть на уровне глаз или чуть ниже. Когда человек смотрит прямо перед собой, его глаза открываются шире, чем, когда он смотрит вниз. За счет этого площадь обзора значительно увеличивается, вызывая обезвоживание глаз. К тому же если экран установлен высоко, а глаза широко открыты, нарушается функция моргания. Это значит, что глаза не закрываются полностью, не омываются слезной жидкостью, не получают достаточного увлажнения, что приводит к их быстрой утомляемости.

Создание благоприятных условий труда и правильное эстетическое оформление рабочих мест на производстве имеет большое значение как для облегчения труда, так и для повышения его привлекательности, положительно влияющей на производительность труда.

4.2.6 Режим труда

Как уже было неоднократно отмечено, при работе с персональным компьютером очень важную роль играет соблюдение правильного режима труда и отдыха. В противном случае у персонала отмечаются значительное напряжение зрительного аппарата с появлением жалоб на неудовлетворенность работой, головные боли, раздражительность, нарушение сна, усталость и болезненные ощущения в глазах, в пояснице, в области шеи и руках.

В таблице 4.5 представлены сведения о регламентированных перерывах, которые необходимо делать при работе на компьютере, в зависимости от продолжительности рабочей смены, видов и категорий трудовой деятельности с ВДТ (видео дисплейный терминал) и ПЭВМ (в соответствии с СанПиНом 2.2.2/2.4.1340-03 «Гигиенические требования к видео дисплейным терминалам, персональным электронно-вычислительным машинам и организации работ») [14].

Таблица 4.5 – Время регламентированных перерывов

Категория работы с ВДТ или ПЭВМ	Уровень нагрузки за рабочую смену при видах работы с ВДТ			Суммарное время регламентированных перерывов, мин	
	Группа А, количество знаков	Группа Б, количество знаков	Группа В, количество часов	При 8-часовой смене	При 12-часовой смене
I	до 20000	до 15000	до 2,0	30	70
II	до 40000	до 30000	до 4,0	50	90
III	до 60000	до 40000	до 6,0	70	120

Примечание. Время перерывов дано при соблюдении указанных Санитарных правил и норм. При несоответствии фактических условий труда требованиям Санитарных правил и норм время регламентированных перерывов следует увеличить на 30%.

В соответствии со СанПиН 2.2.2/2.4.1340-03 все виды трудовой деятельности, связанные с использованием компьютера, разделяются на три группы [14]:

группа А: работа по считыванию информации с экрана ВДТ или ПЭВМ с предварительным запросом;

группа Б: работа по вводу информации;

группа В: творческая работа в режиме диалога с ЭВМ.

Эффективность перерывов повышается при сочетании с производственной гимнастикой или организации специального помещения для отдыха персонала с удобной мягкой мебелью, аквариумом, зеленой зоной и т.п.

4.3 Требования к электробезопасности

4.3.1 Общие требования

Все меры, связанные с обеспечением безопасности эксплуатации электроустановок, делятся на две большие группы:

1) организационные;
2) технические.

К организационным мероприятиям относятся мероприятия, связанные с периодическим медицинским контролем здоровья персонала и выявлением его пригодности к работе на электроустановках.

Лица, обслуживающие и эксплуатирующие электроустановки, относятся к электротехническому персоналу. Электротехнических персонал должен быть физически здоровым, не иметь увечий и болезней, препятствующих выполнению работы. Пригодность к обслуживанию электроустановок определяется при приеме на работу и периодически один раз в два года медицинским освидетельствованием. К работам в электроустановках допускаются лица в возрасте не моложе 18 лет.

Лица, допускаемые к работам в электроустановках, должны иметь соответствующую техническую подготовку. После обучения производится проверка знаний Правил техники безопасности специальной квалификационной комиссией. Проверяемому присваивается квалификационная группа по технике безопасности и

выдается удостоверение, дающее право выполнять определенные работы в соответствии с занимаемой должностью и квалификационной группой.

К мероприятиям технического порядка следует отнести: недоступность токоведущих частей, защитное заземление, защитное зануление, защитное отключение.

4.3.2 Защитное заземление

Защитное заземление – это преднамеренное электрическое соединение с землей или ее эквивалентом металлических нетоковедущих частей, которые могут оказаться под напряжением. Защитное действие заземления основано на снижении напряжения прикосновения при переходе напряжения на нетоковедущей части, что достигается уменьшением потенциала корпуса относительно земли, как за счет малого сопротивления заземления, так и за счет повышения потенциала примыкающей к оборудованию поверхности земли.

При напряжении 380 В и выше переменного и 440 В и выше постоянного тока электроустановки подлежат заземлению во всех случаях. Кроме того, необходимо заземлять корпуса оборудования, установленного в помещениях с повышенной опасностью, особо опасных и в наружных установках с номинальным напряжением выше 42В переменного тока и 110В постоянного тока, а также установленного во взрывоопасных помещениях при всех напряжениях переменного и постоянного тока.

4.3.3 Защитное зануление

Занулением называется преднамеренное электрическое соединение с нулевым защитным проводником металлических нетоковедущих частей, которые могут оказаться под напряжением. Нулевой защитный проводник – это проводник, соединяющий зануляемые части с глухо заземленной нейтральной точкой обмотки источника тока или ее эквивалентом.

Зануление применяется в четырех проводных сетях напряжением до 1000 В заземленной нейтралью.

В сети заземленной нейтралью напряжением до 1000В защитное заземление не эффективно так как ток глухого замыкания на землю зависит от сопротивления заземления. Очевидно, невозможно уменьшить напряжение корпуса, находящегося в комнате с токоведущими частями, устройством заземления с сети с заземленной нейтралью. Другой путь – уменьшить длительность режима замыкания на корпус. Для этого прокладывается дополнительный нулевой провод, соединяющийся с заземленной нейтралью источника и повторными заземлениями. При занулении корпуса электрооборудования соединяются не с заземлителями, а с нулевым проводом. Зануление снижает потенциалы корпусов, появляющиеся в момент замыкания на землю. При замыкании на зануленный корпус, ток короткого замыкания проходит через следующие участки цепи: обмотки трансформатора, фазный провод и нулевой провод.

4.3.4 Организация пожарной профилактики

Противопожарные мероприятия проводятся на основании единых правительственных постановлений, правил и норм, в частности ППБ 01-03 «Правила пожарной безопасности Российской Федерации». В соответствии с ними помещения, в которых проводятся работы с использованием персональных компьютеров, а также сами компьютеры содержат большое количество горючих и легковоспламе-

няющихся материалов, и для того, чтобы не допустить непреднамеренного возгорания, необходимо строго их соблюдать.

Источником возгорания на рабочем месте могут быть провода, электронные схемы ПК, устройства электропитания, сильно нагревающиеся узлы устройств. Поэтому на 100 м^2 площади таких помещений, оборудованных компьютерной техникой должен располагаться минимум 1 огнетушитель углекислого типа.

Все работники организаций должны допускаться к работе только после прохождения противопожарного инструктажа, а при изменении специфики работы проходить дополнительное обучение по предупреждению и тушению возможных пожаров. Руководители организаций или индивидуальные предприниматели имеют право назначать лиц, которые по занимаемой должности или по характеру выполняемых работ должны выполнять соответствующие правила пожарной безопасности.

Государственные органы в пределах своей компетенции реализуют меры пожарной безопасности в подведомственных организациях и на соответствующих территориях, оказывают необходимую помощь пожарной охране.

Во всех производственных, административных, складских и вспомогательных помещениях на видных местах должны быть вывешены таблички с указанием номера телефона вызова пожарной охраны.

В каждой организации распорядительным документом должны быть определены и оборудованы места для курения, определен порядок обесточивания электрооборудования в случае пожара и по окончании рабочего дня, действия работников при обнаружении пожара.

В случае пожара для тушения компьютерной техники необходимо использовать газовые и углекислотные огнетушители. Их достоинством является высокая эффективность тушения пожара и сохранность электронного оборудования.

Использование ПЭВМ в помещениях приводит к принятию серьёзных мероприятий защиты от пожаров, определяемых СП 512-78 «Инструкции по проектированию зданий и помещений для ЭВМ» и СНиП 11-2-80 «Противопожарные нормы проектирования зданий и сооружений» [14]. В этих документах изложены

основные требования к огнестойкости зданий и сооружений, противопожарным преградам, эвакуации людей из зданий и помещений.

Выводы по разделу четыре:

В разделе «Безопасность жизнедеятельности» проведен анализ вредных факторов, оказывающих влияние на органы зрения пользователя ПЭВМ. Сформированы общие требования к помещению и освещению. Проведены анализы шума, электробезопасности, а также пожаробезопасности, на рабочем месте пользователя ПЭВМ.

ЗАКЛЮЧЕНИЕ

В ходе ВКР была подробна изучена тема защита информации от несанкционированного доступа, проведен анализ существующей сети предприятия ООО «СЦСО Надежда», а также изучена необходимость разработки данного программного-аппаратного комплекса СЗИ, согласно Федеральному закону от 26 января 2007 года № 152-ФЗ «О персональных данных», который подразумевает регулирование отношений, связанных с обработкой персональных данных, и устанавливающий требования к защите таких данных [17].

В процессе разработки ВКР было проведено более глубокое изучение предметной области. Получены навыки работы с программно-аппаратным комплексом СЗИ.

В организационно-экономическом разделе ВКР, определены затраты при разработке СЗИ и при ее использовании, определены показатели экономического эффекта.

Таким образом, все поставленные задачи ВКР успешно решены, а разработанный программно-аппаратный комплекс СЗИ соответствует требованиям, изложенным в исходных данных.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — М.: КноРус, 2014. — 136 с.
2. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. — Рн/Д: Феникс, 2014. — 324 с.
3. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. — Ст. Оскол: ТНТ, 2013. — 384 с.
4. Документация InfoWatch EndPoint Security [Электронный ресурс] – режим доступа https://www.infowatch.ru/products/endpoint_security/features. [дата обращения – 25.11.2017]
5. Документация на dallas lock [Электронный ресурс] – режим доступа https://www.dallaslock.ru/products/szi-nsd-dallas-lock/szi-ot-nsd-dallas-lock-8-0-k/[дата обращения – 17.11.2017].
6. Документация на продукты ViPNet [Электронный ресурс] – режим доступа https://infotecs.ru/downloads/documentacii/[дата обращения – 15.11.2017].
7. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга… — М.: ЮНИТИ-ДАНА, 2013. — 239 с.
8. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.1 — Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г Милославская. — М.: ГЛТ, 2015. — 536 с.
9. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 — Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. — М.: ГЛТ, 2013. — 558 с.
10. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. — М.: ГЛТ, 2014. — 280 с.

11. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. — М.: Форум, 2016. — 432 с.

12. Программно-аппаратный комплекс [Электронный ресурс] – режим доступа https://www.securitycode.ru/upload/documentation.pdf [дата обращения – 21.10.2017].

13. СанПиН 2.2.1/2.1.1.1278-03. Гигиенические требования к естественному, искусственному и совмещенному освещению жилых и общественных зданий. – М.: Информационно-издательский центр Минздрава России, 2003. – 112 с.

14. СанПиН 2.2.2/2.4.1340-03. Гигиенические требования к персональным электронно-вычислительным машинам и организации работы. – М.: Информационно-издательский центр Минздрава России, 2003. – 22 с.

15. Семененко, В.А. Информационная безопасность: Учебное пособие / В.А. Семененко. — М.: МГИУ, 2010. — 277 с.

16. Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электронный ресурс] – режим доступа http://www.consultant.ru/document/cons_doc_LAW_208191/#dst0 [дата обращения – 30.10.2017].

17. Федеральный закон «О внесении изменений в главу 5 Федерального закона О персональных данных и статью 1 Федерального закона О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» от 22.02.2017 N 16-ФЗ (последняя редакция) [Электронный ресурс] – режим доступа http://www.consultant.ru/document/cons_doc_LAW_213151 [дата обращения – 29.11.2017].

18. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 25.11.2017) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.01.2018) [Электронный ресурс] – режим доступа http://www.consultant.ru/document/cons_doc_LAW_61798/0e9ec16b786dcbdaaa7f44abfc4a15e601d5be22/#dst100144 [дата обращения – 18.11.2017].

19. Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. — М.: Гелиос АРВ, 2010. — 336 с.

20. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. — М.: ДМК, 2014. — 702 с.

21. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. — М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013. — 416 с.

22. Методические рекомендации по подготовке и оформлению выпускной квалификационной работы (проекта) для технических направлений подготовки 09.03.01 Информатика и вычислительная техника, 09.03.04 Программная инженерия, 12.03.01 Приборостроение, 23.03.01 Технология транспортных процессов / сост. Л.Н.Буйлушкина. - Нижневартовск, 2017. - 35с.

ПРИЛОЖЕНИЕ

ПРИЛОЖЕНИЕ А. КОМПАКТ-ДИСК

Содержание:

1. Пояснительная записка к ВКР
2. Презентация
3. Руководство по настройки и установки СЗИ