Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»
Высшая школа электроники и компьютерных наук
Кафедра «Защита информации»

РАБОТА ПРОВЕРЕНА
Рецензент, нач. отдела ТЗИ и СЭ
ФГУП «ПО «Октябрь»
_____ А.А. Барышев
_____ 2018 г.

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой,
к.т.н., доцент
_____ А.Н. Соколов
_____ 2018 г.

Модернизация системы защиты коммерческой тайны на ФГУП «ПО «Октябрь»

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ – 10.05.03.2018.276.ПЗ ВКР

Консультанты

Безопасность жизнедеятельности,
к.т.н., доцент
_____ Н.В. Глотова
_____ 2018 г.

Руководитель работы,
к.п.н., доцент
_____ О.Р. Уторов
_____ 2018 г.

Автор проекта,
студент группы КЭ-530
_____ В.Е. Щелоков
_____ 2018 г.

Нормоконтролер,
к.т.н., доцент
_____ В.П. Мартынов
_____ 2018 г.

Челябинск 2018

Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»

Высшая школа электроники и компьютерных наук
Кафедра «Защита информации»

Специальность 10.05.03 «Информационная безопасность автоматизированных систем»

УТВЕРЖДАЮ
Заведующий кафедрой
_____ А.Н. Соколов

_____ 2018 г.

З А Д А Н И Е
на выпускную квалификационную работу студента

Щелокова Василия Евгеньевича

Группа ___*КЭ-530*

1. Тема работы

Модернизация системы защиты коммерческой тайны
на ФГУП «ПО «Октябрь»

Утверждена приказом ректора ЮУрГУ от _____ № _____
(утверждена, прот. заседания кафедры от _____ № _____)

2. Срок сдачи студентом законченной работы _____

3. Исходные данные к работе

Отчет о преддипломной практике, нормативно-правовые документы в области защиты информации, документация предприятия-базы практики

4. Содержание расчетно-пояснительной записки (перечень подлежащих разработке вопросов)

4.1 Анализ информационной системы предприятия;

4.2 Нормативно-правовое регулирование в области коммерческой тайны;

4.3 Модернизация системы защиты коммерческой тайны.

5. Перечень графического материала (с точным указанием обязательных чертежей, плакатов в листах формата А1)

Презентация «Модернизация системы защиты коммерческой тайны на ФГУП «ПО «Октябрь» в формате PowerPoint 2013 (pptx)

Количество слайдов -

Всего ___ листов

6. Консультанты по работе (проекту), с указанием относящихся к ним разделов работы (проекта)

Раздел	Консультант	Подпись, дата	
		Задание выдал (консультант)	Задание принял (студент)
Безопасность жизнедеятельности	Н.В. Глотова		

7. Дата выдачи задания _____

Руководитель,
к.п.н., доцент _____ О.Р. Уторов

Задание принял к исполнению _____ В.Е. Щелоков

КАЛЕНДАРНЫЙ ПЛАН

Наименование этапов выпускной квалификационной работы (проекта)	**Срок выполнения этапов работы**	**Отметки о выполнении руководителя**
Введение		
1 Анализ информационной системы предприятия		
2 Нормативно правовое регулирование в области коммерческой тайны		
3 Модернизация системы защиты коммерческой тайны		
4 Безопасность жизнедеятельности		
Заключение		
Библиографический список		
Предзащита ВКР		
Защита ВКР		

Заведующий кафедрой _____ А.Н. Соколов

Руководитель работы _____ О.Р. Уторов

Студент _____ В.Е. Щелоков

АННОТАЦИЯ

Щелоков В.Е. Модернизация системы защиты коммерческой тайны на ФГУП «ПО «Октябрь» – Челябинск: ЮУрГУ, КЭ-530, 83 с., 4 ил., 4 табл., библиогр. список – 12 наим., 7 прил.

Выпускная квалификационная работа выполнена с целью модернизации системы защиты коммерческой тайны ФГУП «ПО «Октябрь»

В выпускной квалификационной работе отражены этапы анализа информационной системы, системы защиты информации, нормативно-правовой базы в области защиты коммерческой тайны и составление списка рекомендаций по модернизации системы защиты.

В процессе выполнения квалификационной работы было проведено предпроектное обследование предприятия, рассмотрены все необходимые документы, регламентирующие порядок защиты информации, а также описывающие информационную систему обработки сведений конфиденциального характера предприятия. Был составлен список рекомендаций по модернизации системы защиты, включающий в себя выбор мер и средств защиты, предотвращающих актуальные угрозы предприятия.

ОГЛАВЛЕНИЕ

СОКРАЩЕНИЯ

АРМ	-	автоматизированное рабочее место;
АС	-	автоматизированная система;
ИБ	-	информационная безопасность;
ИСПДн	-	информационная система персональных данных;
ЛВС	-	локальная вычислительная сеть;
НСД	-	несанкционированный доступ;
ОС	-	операционная система;
ПД ИТР	-	противодействие иностранным техническим разведкам
ПДн	-	персональные данные;
ПО	-	программное обеспечение;
ПЭМИН	-	побочные электромагнитные излучения и наводки;
СЗИ	-	средства защиты информации;
СКЗИ	-	средства криптографической защиты информации;
СЭ	-	специальная экспертиза;
ТЗИ	-	техническая защита информации;

ОПРЕДЕЛЕНИЯ

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению [9].

Доступ к информации, составляющей коммерческую тайну, - ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации [10].

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации [9].

Информация, составляющая коммерческую тайну, - сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны [10].

Коммерческая тайна - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду [10].

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств [9].

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реа-

лизующее контроль за информацией, поступающей в информационную систему и / или выходящей из информационной системы [9].

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами[9].

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин [9].

Обладатель информации, составляющей коммерческую тайну, - лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны [10].

Передача информации, составляющей коммерческую тайну, - передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности [10].

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов [9].

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания [9].

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа [9].

Разглашение информации, составляющей коммерческую тайну, - действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору [10].

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем [9].

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа [9].

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация [9].

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации [9].

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации [9].

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения) [9].

ВВЕДЕНИЕ

В настоящее время, в эпоху информатизации и построения информационного общества, единое информационное пространство становится одним из важнейших признаков и обязательным условием, и характеристикой самого информационного общества.

В России информационное общество начало формироваться в конце XX – начале XXI века. 07 февраля 2008 года Президентом Российской Федерации была утверждена «Стратегия развития информационного общества в Российской Федерации», согласно которой: «Информационное общество характеризуется высоким уровнем развития информационных и телекоммуникационных технологий и их интенсивным использованием гражданами, бизнесом и органами государственной власти» [1].

Современное информационное пространство, в условиях которого функционируют все организации, имеет свои особенности, а именно существенное увеличение объема информации; быстрота поиска, сбора, переработки и представления информации в пригодной форме для ее дальнейшего использования. В этих условиях у руководителей организаций увеличивается потребность в повышении продуктивности аналитической деятельности, в получении более полной и систематизированной информации.

Защита информации, составляющей коммерческую тайну как часть деятельности по обеспечению безопасности предпринимательства в целом, предполагает, что возможны противоправные посягательства на данную информацию, которые могут исходить по различным направлениям. В связи с этим эффективная защита информации должна предусматривать целую систему направлений деятельности, каждому из которых соответствует свой способ защиты.

Следует учитывать мировой опыт по защите информации, составляющей коммерческую тайну. В разных странах существуют различные приоритетные направления защиты информации, составляющей коммерческую тайну. Так, в Германии преобладают законодательные меры, в США и Франции, наряду с ними, предпочтение отдается организации собственных служб безопасности фирм,

для Японии характерен корпоративный дух и долгосрочная занятость в фирме, в Великобритании защита обеспечивается договорными обязательствами.

Таким образом, актуальность нашего исследования обусловлена недостаточно хорошей организацией режима коммерческой тайны, а также проведением аудита информационной безопасности предприятия.

Объектом выпускной квалификационной работы является система защиты информации ФГУП «ПО «Октябрь».

Предметом выпускной квалификационной работы является система защиты сведений, составляющих коммерческую тайну в ФГУП «ПО «Октябрь».

Целью дипломной работы является на основании действующей системы защиты коммерческой тайны выработать предложения по ее модернизации.

В соответствии с поставленной целью необходимо решить следующие задачи:

1. Проанализировать информационную систему предприятия и уровень ее защищенности.
2. Выявить актуальные угрозы и подобрать оптимальные меры для их устранения.
3. Определить модель вероятного нарушителя ИБ.
4. Рассмотреть законодательство в сфере защиты коммерческой тайны и средства защиты информации.
5. Предложить меры по модернизации системы защиты коммерческой тайны в организации.

1. АНАЛИЗ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРЕДПРИЯТИЯ

1.1 Описание предприятия.

Федеральное государственное унитарное предприятие «Производственное объединение «Октябрь» является одним из крупнейших предприятий радиоэлектронного комплекса России. Предприятие занимается выпуском различных изделий - от товаров народного потребления до сложных автоматизированных систем управления. Производство размещено на нескольких промышленных площадках в г. Каменске-Уральском. Право собственности на имущество, составляющее уставной капитал в размере 923 млн. рублей, закреплено за ФСТЭК России.

На предприятии организован выпуск продукции:

- систем радионавигации и радиолокации для всех видов воздушного и морского транспорта;
- радиовысотомеры для самолетов и вертолетов гражданской авиации;
- системы и средства безопасности движения на железнодорожном транспорте;
- оборудование и приборы для нефтяной, газовой промышленности и энергетики;
- соединители радиочастотные и низкочастотные;
- платы печатные односторонние, многослойные и СВЧ-диапазона;
- микросборки СВЧ-диапазона;
- средства УКВ-радиосвязи;
- вычислительную технику специального назначения;
- приборы пожарной безопасности, тренажеры для пожарных
- системы охранной сигнализации, домофоны;
- радиоприемники, абонентские громкоговорители, комплексы громкоговорящей связи;
- изделия из полимерных материалов и резины;
- литые детали для точного машиностроения;
- оснастку и инструменты;

- инвалидные коляски, медицинские приборы и оборудование.

Обобщенная организационная структура предприятия представлена на рисунке 1.

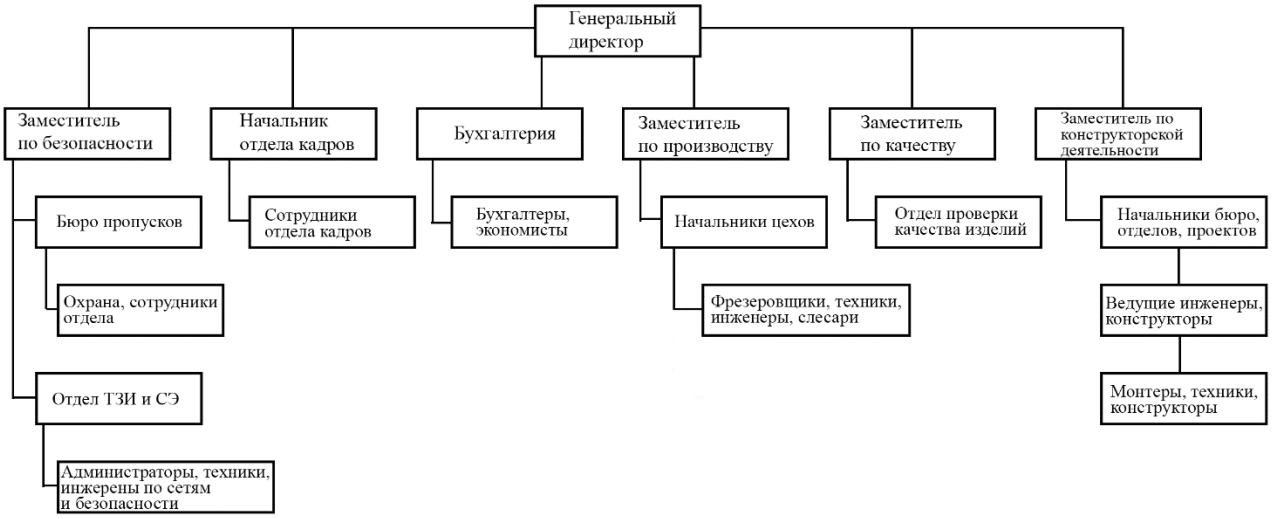

Рис. 1. Обобщенная организационная структура предприятия

Информационная система предприятия состоит из 250 ПЭВМ сотрудников, с опломбированным системным блоком, подключенным к ним принтерами и МФУ; серверного оборудования, установленного в центре обработки данных, которое является специальным помещением; линий связи локальной вычислительной сети предприятия, проложенных с использованием оптоволоконных линий связи в подземных коммуникациях;

В информационной системе используется различное программное обеспечение. Основное, распространенное ПО:

- различные версии ОС Windows;
- офисные пакеты Microsoft Office 2003-2007, LibreOffice 5.2;
- антивирусное Dr.Web 11.0 (сертификат ФСТЭК №3509 до 27.01.2019);
- архивации 7Zip, WinRar;
- защиты информации DeviceLock 8 DLP Suite (сертификат ФСТЭК №3465), VipNet Client 4 (сертификат ФСТЭК №3727 до 30.11.2019, сертификат ФСБ №124-2876 до 31.12.2018);
- профессиональные инструменты Компас-3D, Autodesk AutoCad.

Пользователями программно-аппаратного комплекса информационной системы предприятия являются сотрудники подразделений с разграничением прав к информационным ресурсам.

Схема информационных потоков предприятия подразумевает маршрут движения информации внутри информационной системы предприятия. ПЭВМ сотрудников подразделений имеют прямое подключение к принтерам и МФУ, находящимся в их подразделении и к локальной вычислительной сети предприятия.

При возникновении у работника производственной необходимости в получении информации из сети Интернет или использования электронной почты, он должен составить заявки на доступ к информационным ресурсам или передачу электронной почты, соответственно, в которых указывается пользователь, тип информационного ресурса, краткое содержание почтовых файлов, подпись начальника подразделения о проверке на отсутствие конфиденциальных сведений. Далее, информация полученная из сети Интернет или электронной почты с помощью специального учтенного носителя информации переносится на обособленное АРМ, с целью проверки и обработки информации. После проведения необходимых процедур, с помощью другого учтенного носителя информации полученные сведения заносятся администратором безопасности сети в каталог подразделения в личную папку работника, после чего он может осуществлять обработку информации со своего рабочего места. Обобщенную схему информационных потоков представлена на рисунке 2.

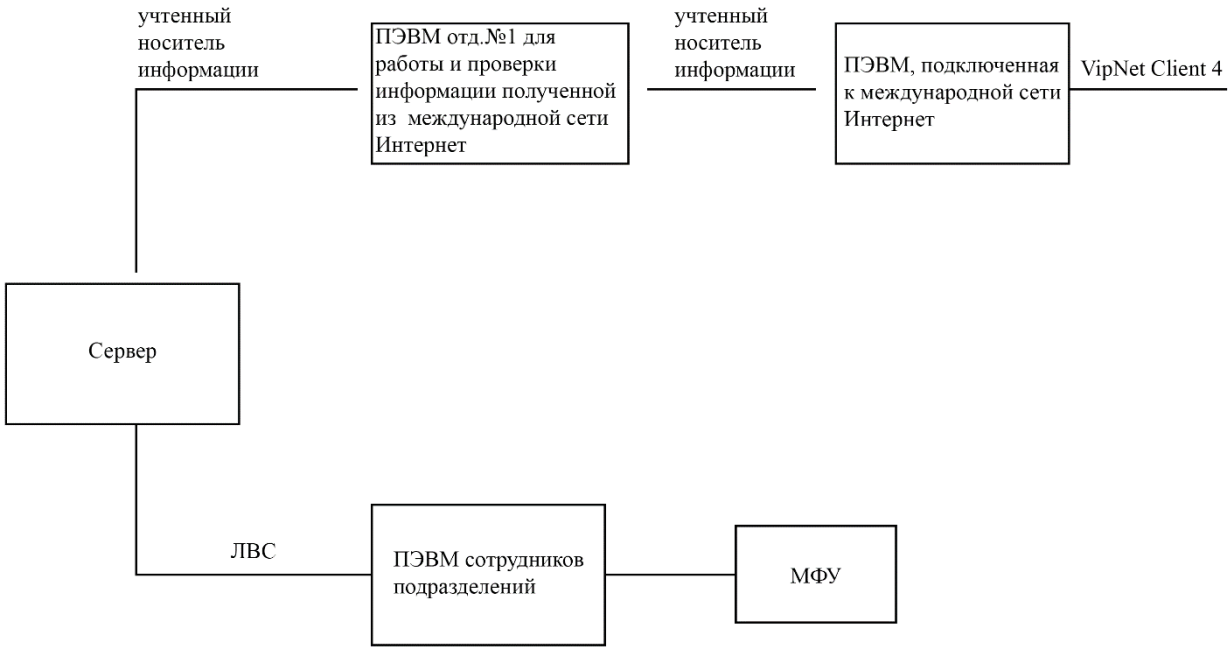

Рис. 2. Обобщенная схема информационных потоков предприятия

При этом локальная вычислительная сеть (ЛВС) предприятия с размещенной в рамках нее информационной системой ограничена внутренним сегментом и не имеет физического подключения к внешней сети Интернет.

Защита информации на предприятии осуществляется специалистами отдела ТЗИ и СЭ, деятельность которых курируют заместитель генерального директора по безопасности и сам генеральный директор. Распорядительная документация основывается на требованиях ФСТЭК России и ФСБ России. Обобщенную схему защиты информации можно наглядно оценить на рисунке 3.

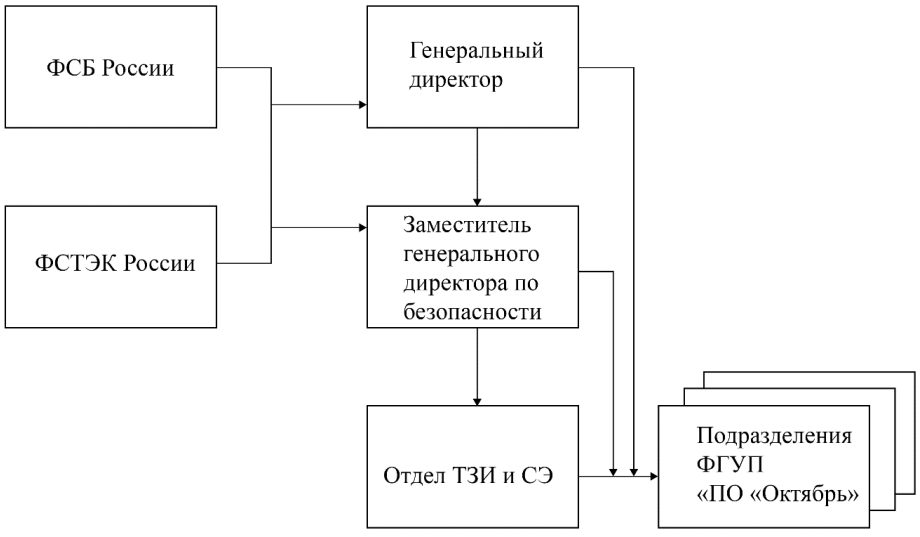

Рис. 3. Схема защиты информации на предприятии

Защита информации на предприятии осуществляется организационными методами (инструктаж о порядке обработки конфиденциальной информации), физической развязкой внутренней (ЛВС) и внешней (Интернет) сетями, дополнительно для защиты канала связи с сетью Интернет применяется межсетевой экран, для предотвращения НСД в ЛВС и автономные ПЭВМ используются программные возможности ОС Windows (с применением парольной политики), прокладка линий связи ЛВС по территории предприятия в подземных коммуникациях или путем подвеса на высоте более 3 метров, прокладка линий связи ЛВС предприятия по корпусам в кабельных лотках, закрепленных между фальш-потолком и потолком.

Дополнительно используются следующие программные и аппаратные средства защиты:

- средство защиты информации от НСД «Страж NT» 3.0 (сертификат ФСТЭК №2145 до 30.07.2019);
- генератор пространственного зашумления «Соната Р2» (сертификат ФСТЭК №1129 до 16.01.2021);
- система виброакустической защиты «Соната-АВ» (модель 1М) (сертификат ФСТЭК №693 до 31.10.2020);
- блокиратор сотовой связи ЛГШ-701 (сертификат ФСТЭК №1252 до 05.09.2021).

1.2 Организационно-правовое обеспечение и кадровая политика.

Правовое обеспечение направлено на разработку и внедрение нормативно-правовой документации, призванной обеспечить предприятие возможностями для ведения деятельности в рамках правового поля. Комплекс мероприятий по внедрению используемых документов на предприятии реализован для достижения следующих целей:

- разработки нормативно-правовой базы;
- анализа и изменения уставных и учетных документов;

- получения лицензий и разрешений для осуществления установленных видов деятельности.

На ФГУП «ПО «Октябрь» разработана и внедрена необходимая нормативно-правовая документация, регулирующая взаимоотношения подразделений, границы обязанностей и ответственности. Основные положения деятельности предприятия, закреплены в Уставе. Имеются лицензии на осуществление деятельности по защите информации в следующих областях:

- проведение анализа организации обеспечения информационной безопасности и режима секретности;

- разработка руководящих документов предприятия по режиму, ПД ИТР и технической защите информации (руководство по защите информации, инструкции по ПД ИТР, инструкции по внутри объектовому режиму и т.д.);

- проведение аттестации объектов информатизации (технических средств передачи и обработки информации, выделенных (защищенных) помещений для проведения закрытых совещаний и т.д.);

- проведение специальных мероприятий по обнаружению устройств негласного съема информации (закладок) в помещениях и технических средствах;

- проведение специальных исследований технических средств передачи и обработки информации (ПЭВМ, средства связи, средств хранения информации и т.д.);

- разработка проектов экранированных сооружений, безэховых камер, выделенных и защищаемых помещений;

- подбор, закупка, монтаж, настройка и сервисное обслуживание средств технической защиты информации;

- подбор, закупка, монтаж, настройка и сервисное обслуживание криптографических устройств;

- проведение аттестации экранированных сооружений, безэховых камер и рабочих мест по требованиям ПД ИТР.

Организационное обеспечение – комплекс мер, направленных на плановое обеспечение потребностей производства и предотвращение возможных инцидентов. Нормативно-правовые документы и сотрудники контролирующих подразделений регулируют соблюдение норм и правил, описанных во внутренней распорядительной документации предприятия.

Кадровое обеспечение регулируется деятельностью отдела кадров. Он отвечает за сбор и регистрацию данных о соискателях вакансий на предприятии. При трудоустройстве соискателем заполняется 2 анкеты: одна по форме 4, так как на предприятии введен режим государственной тайны, другая анкета собственного образца предприятия, где соискатель указывает сведения о себе. После заполнения анкет, претендент на вакансию проходит медицинское обследование у необходимых специалистов (определяется исходя из ст. 212, 213 ТК РФ). В случае утвердительного решения о приеме на работу и отсутствия противопоказаний врача с ним проводят инструктажи по охране труда, пожарной безопасности, внутри объектовому режиму. После чего, уже в рабочее время внутри подразделения проводятся дополнительные локальные инструктажи отдела (цеха), необходимые для работы.

1.3 Коммерческая тайна, обрабатываемая в информационной системе.

На предприятии хранятся и обрабатываются сведения, составляющие коммерческую тайну. Они зафиксированы в перечне сведений коммерческого характера ограниченного распространения ФГУП «ПО «Октябрь». Основными сведениями, составляющие коммерческую тайну, согласно перечня, являются:

- производственная информация: сведения о свойствах и характеристиках материалов и комплектующих изделий, сведения о состоянии производства, сведения о подготовке производства к выпуску новой продукции, сведения о рецептуре материалов, разработанных на предприятии и являющихся собственностью предприятия, сведения о конструкторско-технологических разработках;

- финансовая информация: перечень действующих договоров по выпуску продукции, сведения о производственных мощностях предприятия, сведения об объ-

емах выпуска продукции в натуральном и денежном выражении, сведения о кредитах и долговых обязательствах предприятия, аналитические отчеты об итогах и перспективах реализации продукции, сведения о себестоимости вновь разрабатываемых изделий;

- научно-техническая информация: сведения о методах защиты от подделки продукции и товарного знака предприятия, сведения о патентоведческих исследованиях в области научно-технических, опытно-конструкторских работ, информация оформления патентных формуляров на изобретение;

- информация, составляющая коммерческую тайну сторонних организаций, полученная в ходе деятельности предприятия.

1.4 Техпроцесс обработки коммерческой тайны.

Ввод информации в информационную систему происходит путем занесения данных сотрудником на своем рабочем месте с использованием ПЭВМ и ЛВС через интерфейс пользователя на сервер баз данных, расположенный в ЦОДе.

Под обработкой информации понимается преобразование входной информации к формату, необходимому для ее хранения, преобразование хранимой информации к формату, соответствующему требованиям вывода информации на экран монитора, на печать с использованием принтера или МФУ, или передаче ее непосредственно на производственное оборудование. Обработка информации осуществляется сотрудниками подразделений, как в бумажном, так и в электронном виде с использованием ПЭВМ внутри своего подразделения. Пользователи ПЭВМ имеют разные права доступа к информации, хранящейся как на ПЭВМ, так и на сервере предприятия. Права доступа назначаются администратором безопасности сети штатными средствами серверной ОС и с использованием СЗИ от НСД Страж NT 3.0.

Вывод информации из системы осуществляется на мониторы ПЭВМ, принтера, МФУ и производственное оборудование, подключенное к ЛВС предприятия.

Передача информации в бумажном виде осуществляется собственноручно сотрудниками подразделений. Учет бумажных носителей осуществляется в журнале

учета, табельщиком подразделения, в котором данный носитель был создан (напечатан). При производственной необходимости передачи копии данного носителя сотруднику другого подразделения, на оригинале ставится его подпись, после чего производственные операции выполняются по копии полностью подписанного носителя.

Для файлового обмена информацией в электронном виде между подразделениями предприятия служат каталоги, находящиеся на файловом сервере предприятия. Всем пользователям локальной вычислительной сети предприятия предоставляются полные права для каталога своего подразделения и права на запись для каталогов других подразделений. Сотрудник, забирающий предназначенную для него информацию из каталога своего подразделения, обязан перенести ее на свой компьютер для дальнейшей работы, удалив ее при этом из каталога.

Резервное копирование – процесс создания копии данных на носителе информации, предназначенном для восстановления данных в случае повреждения или разрушения оригинальной информации.

Резервное копирование происходит с периодичностью 1 раз в день. Восстанавливается утраченная информация путем ввода на ПЭВМ данных с сервера, записанных в последнюю сессию резервного копирования. Операции резервирования и восстановления фиксируются в электронном журнале. Бумажные носители восстанавливаются из существующих копий экземпляров или путем повторным распечатыванием утраченного документа.

1.5 Модель вероятного нарушителя информационной безопасности.

Вероятный нарушитель информационной безопасности может быть: внешним, внутренним и комбинированным.

Внешний нарушитель – физическое лицо, не имеющее доступ на территорию предприятия, не сотрудничавшее с предприятием ранее, обладающее информацией о деятельности и структуре предприятия по данным, полученным из открытых источников.

Внутренний нарушитель – физическое лицо, имеющее доступ на территорию предприятия, либо сотрудничающее с предприятием, владеющее информацией о деятельности, структуре, политике информационной безопасности предприятия, полученной из открытых источников и внутренней документацией предприятия.

Комбинированный нарушитель – физическое лицо, ранее имевшее доступ на территорию предприятия, либо ранее сотрудничавшее с предприятием, обладающее информацией о деятельности, структуре, политике информационной безопасности предприятия, полученной из открытых источников и внутренней документацией предприятия.

Для каждого типа вероятного нарушителя существуют свои предположения об имеющейся у него информации:

- для внешнего нарушителя предполагается, что имеется вся информация, необходимая для подготовки и проведения атак, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты информации, а также за исключением сведений:
  - содержание технической документации на технические и программные компоненты средств физического контроля;
  - сведения о линиях связи, нарушениях правил эксплуатации криптосредств и средств физического контроля;
  - сведения о неисправностях и сбои технических средств, криптосредств, средств физического контроля.
- для внутреннего предполагается, что нарушитель обладает информацией об объектах реализации угроз, их защищенности, о структуре предприятия, средствах защиты, топологии сети, организационном обеспечении информационной безопасности. Предполагается, что вероятный нарушитель имеет средства реализации угроз: аппаратные компоненты, криптосредства, технические средства и ПО, находящиеся в свободной продаже, которые возможно незаметно пронести, провезти на территорию предприятия через контрольно-пропускные пункты, либо

замаскированные. Так же предполагается наличие информации о целях реализации угроз информационной безопасности;

- для комбинированного нарушителя предполагается, что он обладает информацией об объектах реализации угроз, их защищенности, о структуре предприятия, установленных средствах защиты, топологии сети, организационном обеспечении информационной безопасности. Предполагается, что вероятный нарушитель имеет средства реализации угроз, возможности которых не превосходят возможности аналогичных средств атак на информацию, содержащую конфиденциальные сведения.

1.6 Модель угроз информационной безопасности коммерческой тайны.

Для составления модели угроз системы защиты, необходимо выявить объекты защиты. Объект защиты – информация, информационный процесс или устройство, которые необходимо защищать с целью сохранности информации. На основании анализа системы защиты коммерческой тайны предприятия составим перечень объектов, нуждающихся в защите:

1. Автоматизированные рабочие места сотрудников.
2. Линии и средства связи.
3. Работники предприятия.
4. Серверное оборудование и помещение.

Для данных объектов защиты был определен уровень исходной защищенности и разработана модель угроз (Приложение А), на основании которых были выявлены актуальные угрозы безопасности:

1. Угрозы утечки видовой информации.
2. Установка ПО, не связанного с исполнением служебных обязанностей.
3. Непреднамеренная модификация, уничтожение информации сотрудниками.
4. Сбой системы электроснабжения.

5. Разглашение, модификация, уничтожение информации сотрудниками, допущенными к ее обработке.

Данные угрозы являются приоритетными для составления рекомендаций по модернизации системы защиты коммерческой тайны на предприятии, с целью устранения угроз информационной безопасности.

1.7 Анализ введенного режима коммерческой тайны.

На ФГУП «ПО «Октябрь» введен режим государственной тайны. Информация, составляющая коммерческую тайну, защищается в соответствии с введенным режимом коммерческой тайны, который регулирует Положение о защите коммерческой тайны ФГУП «ПО «Октябрь». Отсутствующие части в Положении, из соображений достаточности регулирования деятельности подразделений режимными мерами государственной тайны, необходимо восполнить и переработать имеющиеся для полноценного функционирования режима защиты коммерческой тайны.

Необходимо составить список документации для разработки и внедрения, а именно:

1. Граница ответственности лиц, ознакомленных с информацией, составляющей коммерческую тайну.
2. Список лиц, допущенных к информации, составляющей коммерческую тайну.
3. Порядок установления и снятия грифа “Коммерческая тайна”.

Помимо документального сопровождения, требуется ввести организационные меры по оформлению допуска лиц к информации, составляющей коммерческую тайну, усилению контроля доступа к серверному помещению и контролю доступа в режимные подразделения. Ввиду того, что допуск к государственной тайне не является допуском к информации, составляющей коммерческую тайну.

1.8 Вывод по первой части.

В процессе проведения анализа существующей системы защиты коммерческой тайны на ФГУП «ПО «Октябрь» были выявлены объекты защиты, руководствуясь методикой ФСТЭК разработана модель угроз, определен уровень исходной защищенности системы составлен перечень приоритетных к устранению угроз. На основании проведенного анализа системы были получены сведения, необходимые для составления перечня угроз и рекомендаций по их устранению в виде модернизации системы защиты коммерческой тайны. А также описан ряд мер и список организационно-распорядительной документации, необходимой для сопровождения режима коммерческой тайны в должном порядке.

Результатом первой главы является перечень приоритетных к устранению угроз, с помощью которого будут подобраны рекомендации по модернизации системы защиты коммерческой тайны.

2. НОРМАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ В ОБЛАСТИ КОММЕРЧЕСКОЙ ТАЙНЫ

2.1 Законодательство США в области коммерческой тайны

Соединенные Штаты Америки. В США, где существует двухуровневая система законодательства, защита коммерческой тайны регулируется в основном законодательствами штатов (в отличие от таких правовых институтов, как промышленная собственность и авторское право, которые устанавливаются на федеральном уровне). Однако большинство штатов в этом вопросе опираются на единый рамочный законодательный акт (Uniform Trade Secret Act), согласно которому коммерческая тайна определяется как информация (включая формулы, модели, программы, механизмы, способы, технологии), которая обладает самостоятельной экономической ценностью (действительной или потенциальной) и недоступна для других лиц, которые могли бы извлечь экономическую выгоду из ее использования или разглашения, и в отношении которой приняты меры по защите ее секретности. В отличие от объектов патентного права, к коммерческой тайне предъявляются лишь минимальные требования новизны ее содержания. Кроме того, коммерческую тайну может составлять информация, отдельные элементы которой являются общеизвестными, но в совокупности они представляют собой определенную коммерческую ценность.

Отличительной чертой американского законодательства о защите коммерческой тайны является акцент на мерах уголовной ответственности, как наиболее эффективного средства обеспечения прав и интересов обладателя коммерческой тайны. Это объясняется тем, что предусмотренная законом гражданская ответственность (возмещение убытков) не носит достаточного превентивного характера для предотвращения преступлений в этой области. В 1996 году был принят федеральный Закон об экономическом шпионаже (The Economic Espionage Act), согласно которому предусматривается уголовная ответственность за присвоение лицом коммерческой тайны в своих интересах или в интересах третьих лиц, если данное лицо было осведомлено о том, что его действия наносят ущерб обладате-

лю коммерческой тайны, и за приобретение, покупку или владение коммерческой тайной другого лица, переданной или присвоенной без ведома ее обладателя. Под "присвоением" понимается любое незаконное действие (кража, мошенничество, несанкционированное копирование, изготовление чертежей, схем, фотографий, передача файлов и иные виды несанкционированной передачи коммерческой тайны). За посягательства на законные права обладателя коммерческой тайны закон устанавливает наказание в виде лишения свободы сроком до десяти лет и штрафа в размере до полумиллиона долларов США. Если субъектом преступления является юридическое лицо, штраф может доходить до пяти миллионов долларов (в США к уголовной ответственности могут привлекаться юридические лица).

Повышенные наказания предусмотрены также, если кража коммерческих секретов осуществляется в интересах иностранных граждан и организаций. Это объясняется тем, что обеспечение конкурентоспособности национальной экономики является одной из целей защиты коммерческой тайны. Законом также предусматривается конфискация собственности, приобретенной с нарушением прав обладателя коммерческой тайны и, кроме того, использованной для совершения соответствующих правонарушений. Предоставленные федеральным органам власти полномочия по конфискации собственности позволяют им в необходимых случаях производить демонтаж компьютерных сетей, принтеров и другой техники, использованных для совершения преступлений. По закону министр юстиции наделен правом обращаться в суд с гражданским иском о получении судебного запрета в целях защиты законных интересов обладателя коммерческой тайны. Подача таких исков может осуществляться как в рамках уголовного преследования, так и отдельно.

Важным признаком коммерческой тайны в соответствии с Uniform Trade Secret Act является условие о необходимости принятия разумных усилий в целях обеспечения конфиденциальности информации ее обладателем. На практике под "разумными усилиями" понимаются, например, сообщение работникам о необходимости соблюдения режима конфиденциальности определенных сведений, заключение с ними соглашений о неразглашении коммерческой тайны, оборудова-

ние помещений для хранения конфиденциальных документов охранной сигнализацией и т.д. При увольнении работника руководитель компании обычно ставит в известность нового работодателя об осведомленности работника в области коммерческих секретов. Это делается для того, чтобы в дальнейшем иметь возможность требовать возмещения ущерба от компании-нанимателя в случае использования чужих секретов, ведь теперь правонарушителю нельзя сослаться на незнание и неосторожность.

Согласно сложившейся судебной практике, суды не всегда относят к коммерческой тайне информацию, которая, по мнению компании, является коммерчески ценной для осуществления предпринимательской деятельности (даже если это действительно так). Например, клиентская база компании может быть признана коммерческой тайной только тогда, когда внесенные в нее клиенты не известны в соответствующей отрасли предпринимательства и могут быть установлены только с применением значительных организационных и финансовых ресурсов, кроме того, необходимым для признания условием являются большие затраты времени на создание базы. В этом случае возможно доказать коммерческую ценность клиентской базы на основании отсутствия аналогичной информации у конкурентов.

Специфической чертой является широкое применение в частном секторе и в ходе судебных разбирательств полиграфных проверок (с использованием детектора лжи). Это позволяет службам безопасности коммерческих компаний эффективно бороться с экономическим шпионажем и предотвращать значительное количество утечек конфиденциальной информации. В настоящее время количество полиграфных проверок превышает 4 миллиона в год.

2.2 Европейское законодательство в области коммерческой тайны

Несмотря на то, что все государства-члены Европейского Союза (далее — ЕС) являются участниками Соглашения по торговым аспектам прав интеллектуальной собственности (далее — Соглашение ТРИПС), которое, в свою очередь, в соответствии со статьей 39, устанавливает минимальные требования к защите закрытой информации от незаконного получения, использования или раскрытия, в

законодательствах государств-членов ЕС в настоящее время существуют важные различия в объеме и уровне защиты, предоставляемой такой информации, а также разные требования отнесения информации к той или иной категории закрытой информации.

На практике активно используются такие категории закрытой информации как: «коммерческая тайна», «секрет производства», «ноу-хау» и «деловая информация». Существенные различия в отнесении информации к тому или иному виду коммерчески значимой информации в разных государствах-членах ЕС связаны с отсутствием единого понимания по данному вопросу. Все это приводит к тому, что в отношении одной и той же информации в разных государствах-членах ЕС установлен разный уровень защиты.

Такое положение дел снижает трансграничную деятельность на территории ЕС, связанную с инновационным и научно-исследовательским сотрудничеством, аутсорсингом, производственными кооперациями и инвестированием, в процессе которых происходит предоставление или передача закрытой информации, что, в свою очередь, приводит к фрагментации внутреннего рынка ЕС.

В целях сближения законодательств государств-членов ЕС в сфере обращения с закрытой информацией и установления на всей территории ЕС сопоставимого уровня защиты такой информации от незаконного получения, использования или разглашения ЕС была разработана и в июне 2016 г. утверждена Директива 2016/943 о защите нераскрытых ноу-хау и деловой информации (коммерческой тайны) от незаконного получения, использования и разглашения (далее — Директива), которая на законодательном уровне закрепляет понятие коммерческой тайны и устанавливает общие правила ее защиты. При этом Директива позволяет государствам-членам ЕС предусматривать в своих законодательствах более обширные способы защиты коммерческой тайны.

Директива вступила в силу 5 июля 2016 г.

И так, данная Директива вводит понятие «коммерческая тайна», определяет, что является законным и незаконным получением, использованием и разглашением коммерческой тайны, устанавливает меры и средства судебной

защиты при незаконном получении, использовании или разглашении коммерческой тайны.

В соответствии со статьей 2 Директивы под коммерческой тайной понимается информация, которая удовлетворяет всем следующим требованиям:

- является секретной в том смысле, что она в целом или в определенной конфигурации и подборе ее компонентов не является общеизвестной или легко доступной лицам в определенных кругах, которые обычно имеют дело с подобной информацией;

- она имеет коммерческую ценность, поскольку она секретна;

- в отношении такой информацией лицом, правомерно владеющим ею, приняты разумные меры для сохранения ее в секрете.

Как мы видим, данное определение коммерческой тайны практически повторяет определение закрытой информации, приведенное в Соглашении ТРИПС.

В Декларативной части Директивы отмечено, что такое определение коммерческой тайны охватывает ноу-хау, деловую информацию и техническую информацию, в случае если такая информация соответствует установленным требованиям и у ее обладателя имеется законное право сохранить ее в секрете. Вместе с тем в Декларативной части Директивы отмечено, что на ноу-хау и информацию, охраняемую в качестве коммерческой тайны, не распространяется исключительное право.

Ни в Декларативной части Директивы, ни в самой Директиве не определен перечень «разумных мер», которые обладатель коммерческой тайны должен принять для сохранения ее в секрете. Таким образом, данные меры носят субъективный характер и зависят от обстоятельств.

В статьях 3-4 Директивы определены способы правомерного и незаконного получения, использования и разглашения коммерческой тайны.

Статья 8 Директивы предписывает государствам-членам установить срок исковой давности при условии, что он не должен превышать 6 лет.

В статье 10 Директивы перечислены временные и обеспечительные меры, которые судебные органы могут назначить в отношении предполагаемого нарушителя.

В случае установления судебными органами факта незаконного получения, использования или разглашения коммерческой тайны, по желанию заявителя судебные органы в целях предотвращения такого получения, использования или разглашения могут назначить в отношении нарушителя запретительные меры, которые приведены в статье 12 Директивы, а также корректирующие меры в отношении контрафактных товаров. Вместе с тем по заявлению пострадавшей стороны судебные органы могут назначить нарушителю возмещение обладателю коммерческой тайны убытков, причиненных в результате незаконного приобретения, использования или разглашения коммерческой тайны. Порядок определения убытков приведен в статье 14 Директивы.

Также необходимо отметить, что Директива предусматривает положения, запрещающие участникам судебного разбирательства, предметом которого является незаконное получение, использование или разглашение коммерческой тайны, использовать или разглашать такую коммерческую тайну.

Таким образом, согласно статье 19 Директивы государства-члены ЕС должны до 9 июня 2018 г. привести свое национальное законодательство в соответствие с положениями Директивы. Они могут предусмотреть в своих законодательствах более обширные способы защиты коммерческой тайны, дополнительно определить некоторые термины и заполнить пробелы, выбрав допустимый вариант. (на данный момент соответствующая база предложена или уже внедрена в таких странах, как Латвия)

2.3 Законодательство Российской Федерации в области защиты информации, составляющей коммерческую тайну

В Российской федерации основным законом, регламентирующим отношения с информацией, составляющей коммерческую тайну является федеральный закон № 98 “О коммерческой тайне”, который был разработан и внедрен в действие

29.07.2004 г. Он устанавливает понятие коммерческой тайны и право на ее сохранность.

209-ФЗ "О развитии малого и среднего предпринимательства" также имеет положения, касающиеся информации, составляющей коммерческую тайну. Статья 5 регламентирует предоставление сведений, составляющих коммерческую тайну. Держатель обязан по требованию органов государственных властей либо муниципальных, предоставить сведения, входящие в понятие коммерческой тайны. Прошение должно быть удостоверено подписью должностного лица, с определением права и цели запроса сведений, и период их подачи, если он не регламентирован законодательством;

Если держатель данных отказывается предоставлять информацию органам государственной власти или муниципальным органам, они имеют основание запросить их через суд;

Держатель коммерческой тайны и государственные органы, и иные организации, имеющие доступ к коммерческой тайне, обязаны предоставить сведения по требованию судебных инстанций, следственных и спецслужб, по системе и праву, прописанным в законах РФ.

На акты, где указана коммерческая тайна, наносится отметка «Коммерческая Тайна», с обозначением сведений о ее владельце.

Статья 10 содержит данные об охране конфиденциальности сведений. Прописывает способы охраны коммерческой тайны, порядок установления режима коммерческой тайны, установление о том, что помимо способов защиты, прописанных в п.1 статьи, владелец может использовать механические способы сохранить тайну данных, и любые другие, не нарушающие законодательства страны.

2.4 Предложение поправок к законодательству

Так как коммерческая тайна не имеет сильного государственного регулирования, то необходимо чтобы органы власти (например, правоохранительные органы или налоговая инспекция) получившие доступ к информации организации, составляющей коммерческую тайну в ходе проведения расследований, осуществля-

ли сохранность данной информации на том же уровне, что и правообладатель данной информации.

Законом предусмотрена обязанность организаций по запросам налоговых, природоохранных, антимонопольных и других государственных органов предоставлять информацию, составляющую коммерческую тайну, необходимую для решения стоящих перед ними задач. Вместе с тем процедура передачи информации закреплена в некоторых правовых актах, определяющих правовое положение федеральных министерств и служб. Статья 6 98-ФЗ устанавливает обязанность обладателя предоставлять такую информацию по требованию органов государственной власти, иного государственного органа, органа местного самоуправления. По моему мнению, правом получения информации, содержащей коммерческую тайну, должны быть наделены только те государственные органы, которые выполняют судебные, надзорные и контрольные функции по отношению к организациям и индивидуальным предпринимателям на основании федерального закона. Полагаю, что предоставление данных полномочий всем государственным органам власти и управления, их должностным лицам, включая и местные органы власти, на изъятие информации, содержащей коммерческую тайну, не будет способствовать реализации конституционного принципа равенства защиты частной и государственной собственности [12].

2.5 Сравнение популярных антивирусных средств защиты информации

Главное предназначение антивирусной программы – это защита информации, которая хранится на компьютере от компьютерных вирусов.

Кроме защиты компьютера антивирус проверяет посещаемые Вами интернет сайты и в случае обнаружения на сайте нежелательного ПО блокирует его. Так же антивирус убирает с большинства сайтов надоедливую рекламу.

Еще одна очень важная функция – это «Родительский контроль». Антивирус позволяет ставить запрет на посещение определенных сайтов.

Существует два основных пути заражения компьютера:

- скачивание, каких-либо зараженных файлов с Интернета.

- через съемные носители. Когда вирус уже присутствует на носителе и вовремя копирования информации он перемещается на компьютер.

Однозначного ответа какую антивирусную программу выбрать нет. Каждая программа имеет свои плюсы и минусы. Поэтому выбор остается только за конечным потребителем исходя из его предпочтений.

Какие функции должен иметь антивирус.

Набор обязательных функций, которые должны быть в наличии для корректной защиты компьютера.

1) Антивирусный мониторинг. Проверка папок и файлов, которые используются в данный момент на наличие вирусов.

2) Сканер. Опция, которая позволяет проводить проверку жестких дисков компьютера на присутствие вирусов.

3) Автозащита. Некоторые вирусы пытаются отключить работу антивируса, что бы этого не случилось, антивирус должен иметь автозащиту.

4) Контроль работы программ. Если программа заражается вирусом, то процесс ее работы начинает меняться что и должен сразу обнаружить антивирус.

5) Сетевой и интернет контроль. Важная функция, которая отвечает за работу компьютера в локальной сети или в Интернете.

6) Обновление антивирусных баз. Учитывая то, что новые вирусы появляются чуть ли не каждый день, антивирус должен регулярно обновлять свою базу вирусов, чтобы максимально защитить компьютер.

7) Ресурсопотребление. Лучше выбирать антивирусы с низким потреблением ресурсов компьютера. Чем данный показатель ниже, тем комфортнее работать за ПК.

Ниже приведено описание самых распространённых антивирусных программ.

Антивирус Касперского.

Самый популярный российский антивирус. Имеет две вариации: Антивирус Касперского и Kaspersky Internet Security. Отличие между ними в том, что второй вариант помимо стандартной защиты ПК имеет еще и интернет-защиту что является важным плюсом.

Плюсы данной программы:

- высокая защита;
- множество дополнительных функций;
- широкие возможности настроек.

Минусы программы:

- высокая стоимость лицензии;
- жесткий контроль процессов других программ.

Dr.Web.

Антивирус занимает второе место по популярности и так же производится в России. Выпускается в двух версиях: простая и с интернет защитой. В сравнении с Антивирусом Касперского, Dr.Web немного проигрывает, как по количеству функции, так и по качеству защиты.

Avast Free Antivirus

Прекрасный бесплатный антивирус чешского производства. Имеет довольно хорошую защиту от вирусов как для бесплатного антивируса. Регулярно обновляет свою базу данных вирусов, что гарантирует максимальную защиту ПК.

NOD32

Производится в Словакии с 1987 года. Хороший антивирус главным преимуществом, которого есть малое потребление системных ресурсов компьютера. Существует так же расширенная версия антивируса NOD32 Smart Security, которая обеспечит надежную защиту компьютера при работе в интернете.

Каждый антивирус имеет как плюсы, так и минусы. Все зависит от предпочтений пользователя, имеющихся финансовых ресурсов, производительности компьютера. Нужно понимать, что нет антивируса с гарантированной стопроцентной защитой и возможность заразить компьютер остается всегда.

2.6 Выводы по второй части.

В данной части работы было рассмотрено нормативно-правовое регулирование коммерческой тайны в США, Европе и Российской Федерации, после чего были предложены поправки к существующему законодательству РФ в области

защиты информации. А также проведен анализ популярного антивирусного программного обеспечения с выявлением достоинств и недостатков по результатам тестов и личного опыта из открытых источников информации.

3. МОДЕРНИЗАЦИЯ СИСТЕМЫ ЗАЩИТЫ КОММЕРЧЕСКОЙ ТАЙНЫ

3.1 Введение.

На предприятии ФГУП «ПО «Октябрь» осуществляется комплекс мер по защите информации, обрабатываемой в информационной системе. По результатам составленной модели угроз были выявлены актуальные угрозы, защищенность от которых необходимо повысить. Поэтому предлагается ряд мер, для повышения уровня защищенности от возможных угроз.

3.2 Организационные меры.

С целью повышения защищенности от угроз типа: Угрозы утечки видовой информации; разглашение, модификация, уничтожение информации сотрудниками, допущенными к ее обработке, рекомендуется ввести определенные организационные меры:

1. Проведение информирования об обновлении законодательства в сфере информационной безопасности.
2. Проведение плановых осведомлений об ответственности за нарушение законодательства, уставов и политик предприятия с приведением статистики по произошедшим инцидентам.
3. Оснащение окон кабинетов сотрудников, находящихся на первом этаже заводоуправления металлическими решетками.
4. Оснащение серверного помещения стационарными RFID-считывателями, по типу уже установленных в некоторых подразделениях предприятия.
5. Оснащение режимных подразделений турникетов с RFID считывателем, по типу уже установленных на предприятии.

Предполагается, что данные меры инструктажа позволят повысить информированность, дисциплинированность и ответственность сотрудников предприятия и снизить частоту возникновения инцидентов информационной безопасности. А

меры, направленные на контроль доступа в режимные и серверные помещения, позволит ограничить угрозы утечки видовой информации.

3.3 Управление правами доступа.

На предприятии ФГУП «ПО «Октябрь» реализовано ограничение прав пользователей на установку стороннего программного обеспечения. Такими правами обладают администраторы информационной безопасности, администраторы вычислительной сети и сотрудники подразделения по техническому обслуживанию вычислительной техники.

Для повышения защищенности системы от возможных программных уязвимостей, вредоносного ПО, рекомендуется ограничить права на выполнение сторонних исполняемых файлов-инсталлеров и скриптов средствами ОС Windows. Распространить права рекомендуется только на администраторов информационной безопасности. А также обеспечить документирование данной процедуры путем запроса на установку стороннего программного обеспечения через служебную записку и акт установки программного обеспечения, оформляемый администратором. В связи с реорганизацией обязанностей администраторов необходимо разработать обновленную инструкцию. Соответствующие образцы документов были разработаны и готовы к внедрению (Приложение Б, В, Г).

3.4 Резервное копирование.

В информационной системе предприятия реализовано плановое резервное копирование ключевых элементов информационной системы с сервера баз данных на выделенное дисковое хранилище с периодичностью 1 раз в день.

Для поддержания работоспособности системы в случае утраты/модификации информации рекомендуется:

- включить в план резервного копирования информацию с ПЭВМ руководителей подразделений;
- увеличить внутреннее пространство дискового хранилища, путем приобретения дополнительных жестких дисков.

Для анализа с целью расширения дискового пространства хранилища резервного копирования были выбраны три продукта категорий жестких дисков, представленных на рынке:

1. HGST Ultrastar HE12
2. SEAGATE Ironwolf 12Тб
3. WD Gold WD121KRYZ

Таблица 1. Оценка характеристик жестких дисков.

Устройство / Параметр	HGST HUH721212ALE604	SEAGATE Ironwolf 12Tb	WD Gold WD121KRYZ
Средняя цена на рынке, руб	21810	25857	29500
Наработка на отказ, ч	2500000	1000000	2500000
Уровень шума при работе, дБ	36	32	36
Уровень шума простоя, дБ	20	28	20
Потребляемая мощность, Вт	7,2	7,8	6,9
Гарантия производителя, мес	60	36	60
Объем накопителя, Тб	12	12	12

По результатам анализа характеристик, перечисленных в таблице был выбран жесткий диск HGST HUH721212ALE604.

3.5 Источники бесперебойного питания.

Предприятие ФГУП «ПО «Октябрь» подключено к электросети городского снабжения с трансформаторной подстанцией, размещенной в пределах контролируемой зоны предприятия. С целью ликвидации угрозы сбоя системы электроснабжения рекомендуется оборудовать ключевые элементы информационной системы источниками бесперебойного питания (ИБП). ИБП защищает технику от скачков напряжения и вызванных ими отказов оборудования, обеспечивает надежность и стабильность работы электроники.

Для анализа характеристик было выбрано три устройства из различных ценовых категорий, их сравнение приведено в таблице 2.

Таблица 2. Характеристики источников бесперебойного питания.

Устройство / Параметр	CyberPower CP900EPFCLCD	CyberPower CP1300EPFCLCD	Ippon Back Comfo Pro 1000 New
Цена, руб	10243	13660	6850
Выходная мощность, Вт	540	780	600
Время работы при полной и половинной нагрузке, мин	1 и 7	2 и 9	3 и 30
Максимальная поглощаемая энергия импульса, Дж	405	405	320
Количество разъемов питания	6	6	8
Отображение информации	ЖК-экран	ЖК-экран	Светодиодные индикаторы
Тип предохранителя	плавкий	плавкий	автоматический

Проанализировав все характеристики устройств, был выбран источник бесперебойного питания Ippon Back Comfo Pro 1000 New, ввиду его экономичности типа предохранителя, достаточной выходной мощности для обслуживания ключевого узла информационной системы и ценового превосходства относительно других.

3.6 Вывод по третьей части.

Таким образом, на основании анализа системы, составленной модели угроз и выявленных актуальных угроз информационной безопасности для предприятия ФГУП «ПО «Октябрь» был сформирован список рекомендаций для модернизации существующей системы защиты. Для защиты от актуальных угроз предложены меры:

- проведение дополнительных инструктажей по работе, ответственности и обновлению законодательства в сфере защиты информации и оснащение RFID считывателями серверного помещения;
- уменьшение категорий пользователей, с правами на установку стороннего программного обеспечения;
- увеличение элементов системы, для резервного копирования, а также увеличение дискового пространства хранилища резервных копий за счет жестких дисков типа HGST HUH721212ALE604;
- установка источников бесперебойного питания Ippon Back Comfo Pro 1000 New во все ключевые узлы системы.

Часть необходимой документации была разработана, переработана и приложена к работе.

4. БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

Раздел безопасность жизнедеятельности описывает систему норм и мероприятий, необходимых для создания безопасных условий труда. Включает в себя организацию рабочего пространства, контроль освещенности и проветриваемости помещения, регламентацию по режиму работы и отдыха, элементы электро- и пожарной безопасности.

Рассмотрим основные нормативные документы и приведем некоторые рекомендации по организации рабочего места пользователя.

4.1 Рекомендации по выбору помещения для размещения рабочего места.

При работе с вычислительной техникой важным фактором, обеспечивающим высокий уровень работоспособности, является правильно спроектированное помещение, в котором будут располагаться рабочие места, оборудование ЭВМ с ВДТ.

По требованиям СанПиН 2.2.2/2.4.1340-03 [5] помещения для эксплуатации ПЭВМ должны отвечать следующим требованиям:

– помещения должны иметь естественное и искусственное освещение;

– естественное и искусственное освещение должно соответствовать требованиям действующей нормативной документации;

– площадь на одно рабочее место пользователей ПЭВМ с ВДТ на базе плоских дискретных экранов (жидкокристаллические, плазменные), по СанПиН 2.2.2/2.4.1340-03, должно быть– 4,5 м^2 и 6 м^2 для ВДТ на базе ЭЛТ;

– для внутренней отделки интерьера помещений, где расположены ПЭВМ, должны использоваться диффузно-отражающие материалы с коэффициентом отражения для потолка – 0,7−0,8; для стен – 0,5−0,6; для пола – 0,3−0,5;

– помещения, где размещаются рабочие места с ПЭВМ, должны быть оборудованы защитным занулением или заземлением в соответствии с техническими требованиями по эксплуатации;

– не допускается расположение рабочих кабинетов, оборудованных ПЭВМ, в полуподвальных и подвальных помещениях.

Не следует размещать рабочие места с ПЭВМ вблизи силовых кабелей и вводов, высоковольтных трансформаторов, технологического оборудования, чтобы избежать появления помех, нарушающих функционирование ПЭВМ.

4.2 Требования к микроклимату.

Для рабочих мест, на которых работа с ПЭВМ является основным видом выполняемых работ и связана с непрерывным эмоциональным напряжением, согласно СанПиН 2.2.2/2.4.1340-03 должны быть обеспечены оптимальные параметры микроклимата для работ категории Iа (Таблица 3). Параметры требований к микроклимату для работ различных категорий приведены в СанПиН 2.2.4.3359-16 [6].

Таблица 3. Гигиенические требования к микроклимату производственных помещений (СанПиН 2.2.4.3359-16).

Период года	Категория работ по уровням энергозатрат, Вт	Температура воздуха, °С	Температура поверхностей, °С	Относительная влажность воздуха, %	Скорость движения воздуха, м/с
Холодный	Iа (до 139)	22 – 24	21 – 25	60 – 40	0,1
Теплый	Iа (до 139)	23 – 25	22 – 26	60 – 40	0,1

В соответствии с СанПиНом 2.2.4.3359-16, в помещениях, оборудованных ПЭВМ, должна проводиться ежедневная влажная уборка, а также проветривание после каждого часа работы на ПЭВМ.

4.3 Требования к уровням шума.

При работе на ПЭВМ источниками шума являются:

– источник бесперебойного питания;

– системный блок ПЭВМ;

– работающие принтеры и многофункциональные устройства.

Уровень шума на рабочих местах, при выполнении основных и вспомогательных производственных работ с использованием ПЭВМ не должен превышать показателей, устанавливаемых нормами СанПиН 2.2.2/2.4.1340-03 предельно допустимых значений для данных видов работ в соответствии с действующими санитарно-эпидемиологическими нормативами. А именно должен соответствовать нормам СанПиН 2.2.4.3359-16 для высококвалифицированной работы, требующей сосредоточенности, в рабочих комнатах.

В соответствии с нормами, ограничивающими предельно допустимое звуковое давление для рабочих мест, оснащенных ПЭВМ: шумящее оборудование, уровни шума которого превышают нормативные, должно размещаться вне помещений с ПЭВМ.

В соответствии с СанПин 2.2.4.3359-16 уровни шума на рабочих местах не должны превышать 80дБА.

4.4 Требования к освещению.

При работе с вычислительной техникой важным фактором, обеспечивающим высокий уровень работоспособности, является правильно спроектированное освещение, не вызывающее раннего переутомления. Работа программиста требует большой зрительной нагрузки, поэтому необходимо применять естественное освещение совместно с искусственным.

Согласно СанПиН 2.2.2/2.4.1340-03 рабочие столы следует размещать таким образом, чтобы ВДТ были ориентированы боковой стороной к световым проемам, чтобы естественный свет падал преимущественно слева. Искусственное освеще-

ние в помещениях для эксплуатации ПЭВМ должно осуществляться системой общего равномерного освещения. В производственных и административно-общественных помещениях, в случаях преимущественной работы с документами и бумагами, следует применять системы комбинированного освещения.

Освещенность на поверхности рабочего стола должна быть 300−500 лк. Освещенность поверхности экрана не должна быть более 300 лк., освещение не должно создавать бликов на поверхности экрана.

Для освещения помещений с ПЭВМ рекомендуется применять светильники с зеркальными параболическими решетками, укомплектованными электронными пускорегулирующими аппаратами (ЭПРА). Общее освещение при использовании люминесцентных светильников следует выполнять в виде сплошных или прерывистых линий светильников, расположенных сбоку от рабочих мест, параллельно линии зрения пользователя и линии оконных проемов при рядном расположении рабочих мест, оснащенных ПЭВМ с ВДТ. При периметральном расположении компьютеров линии светильников должны располагаться локализовано над рабочим столом ближе к его переднему краю, обращенному к оператору. Коэффициент пульсации не должен превышать 5%.

Для обеспечения нормируемых значений освещенности в помещениях для использования ПЭВМ следует проводить чистку стекол оконных рам и светильников не реже двух раз в год и проводить своевременную замену перегоревших ламп.

4.5 Общие требования к организации рабочих мест.

Рабочее место оператора ЭВМ проектируется согласно СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы».

При размещении рабочих мест с ПЭВМ расстояние между рабочими столами с видеомониторами (в направлении тыла поверхности одного видеомонитора и экрана другого видеомонитора), должно быть не менее 2,0 м, а расстояние между боковыми поверхностями видеомониторов – не менее 1,2 м.

Рабочие места с ПЭВМ в помещениях с источниками вредных производственных факторов должны размещаться в изолированных кабинах с организованным воздухообменом.

Рабочие места с ПЭВМ при выполнении работы, требующей значительного умственного напряжения или высокой концентрации внимания, рекомендуется изолировать друг от друга перегородками высотой 1,5−2,0 м.

Экран видеомонитора должен находиться от глаз пользователя на расстоянии 600−700 мм, но не ближе 500 мм с учетом размеров алфавитно-цифровых знаков и символов.

Конструкция рабочего стола должна обеспечивать оптимальное размещение на рабочей поверхности используемого оборудования с учетом его количества и конструктивных особенностей, характера выполняемой работы.

При этом допускается использование рабочих столов различных конструкций, отвечающих современным требованиям эргономики. Поверхность рабочего стола должна иметь коэффициент отражения 0,5−0,7.

При организации рабочих мест необходимо использовать рабочий стул (кресло) обеспечивающий поддержание рациональной рабочей позы при работе на ПЭВМ, позволяющий изменять позу с целью снижения статического напряжения мышц шейно-плечевой области и спины для предупреждения развития утомления. Тип рабочего стула (кресла) следует выбирать с учетом роста пользователя, характера и продолжительности работы с ПЭВМ.

Рабочий стул (кресло) должно быть обеспеченно подъемно-поворотным механизмом, также оно должно быть регулируемым по высоте и углам наклона сиденья и спинки, а также расстояния спинки от переднего края сиденья, при этом регулировка каждого параметра должна быть независимой, легко осуществляемой и иметь надежную фиксацию.

Поверхность сиденья, спинки и других элементов стула (кресла) должна быть полумягкой, с нескользящим, слабо электризующимся и воздухопроницаемым покрытием, обеспечивающим легкую очистку от загрязнений.

Высота рабочей поверхности стола должна регулироваться в пределах 680−800 мм; при отсутствии такой возможности высота рабочей поверхности стола должна составлять 725 мм.

Модульными размерами рабочей поверхности стола для ПЭВМ, на основании которых должны рассчитываться конструктивные размеры, следует считать: ширину 800, 1000, 1200 и 1400 мм, глубину 800 и 1000 мм при нерегулируемой его высоте, высота должна быть равной 725 мм.

Рабочий стол должен иметь пространство для ног высотой не менее 600 мм, шириной – не менее 500 мм, глубиной на уровне колен – не менее 450 мм и на уровне вытянутых ног – не менее 650 мм.

Конструкция рабочего стола должна обеспечивать оптимальное размещение на рабочей поверхности используемого оборудования с учетом его количества и конструктивных особенностей (размер ВДТ и ПЭВМ, клавиатуры, и др.), характера выполняемой работы. При этом допускается использование рабочих столов различных конструкций, отвечающих современным требованиям эргономики.

Конструкция стула (кресла) должна обеспечивать:

- ширину и глубину поверхности сиденья не менее 400 мм;
- поверхность сиденья с закругленным передним краем;
- регулировку высоты поверхности сиденья в пределах 400−550 мм и углам наклона вперед до 15°, и назад до 5°;
- высоту опорной поверхности спинки 300±20 мм, ширину – не менее 380мм и радиус кривизны горизонтальной плоскости – 400 мм;
- угол наклона спинки в вертикальной плоскости в пределах ±30°;
- регулировку расстояния спинки от переднего края сиденья в пределах 260−400 мм;
- стационарные или съемные подлокотники длиной не менее 250 мм и шириной – 50−70 мм;
- регулировку подлокотников по высоте над сиденьем в пределах 230±30 мм и внутреннего расстояния между подлокотниками в пределах 350−500 мм.

Рабочее место пользователя ПЭВМ, согласно СанПиН 2.2.2.542-96 [10], следует оборудовать подставкой для ног, имеющей ширину не менее 300 мм, глубину не менее 400 мм, регулировку по высоте в пределах до 150 мм и по углу наклона опорной поверхности подставки до 20°. Поверхность подставки должна быть рифленой и иметь по переднему краю бортик высотой 10 мм.

Клавиатуру следует располагать на поверхности стола на расстоянии 100−300 мм от края, обращенного к пользователю или на специальной, регулируемой по высоте рабочей поверхности, отделенной от основной столешницы.

4.6 Электробезопасность.

По степени опасности поражения электрическим током согласно Правилам Устройства Электроустановок (ПУЭ) рабочее помещение относится к классу помещений с повышенной опасностью, так как имеется возможность одновременного прикосновения человека к имеющим соединения с землей металлоконструкциям здания с одной стороны и металлическим корпусам электрооборудования с другой.

Если физический доступ к токоведущим частям оборудования затруднен, то основной причиной возникновения данного опасного фактора может являться прикосновение к металлическим нетоковедущим частям (например, корпусу ПЭВМ), которые могут оказаться под напряжением в результате повреждения изоляции. В соответствии с правилами электробезопасности, должен осуществляться постоянный контроль состояния электропроводки, предохранительных щитов, шнуров, с помощью которых включаются в электросеть компьютеры, осветительные приборы, другие электроприборы.

Для защиты от случайного прикосновения к металлическим нетоковедущим частям оборудования, которые могут оказаться под напряжение применяют следующие меры:

- защитное заземление;
- зануление;
- изоляцию нетоковедущих частей;

- защитное экранирование.

Данные меры описаны в ГОСТ Р 12.1.019-2009 «ССБТ. Электробезопасность. Общие требования и номенклатура видов защиты» [3].

4.7 Пожарная безопасность.

Горючие вещества и материалы, находящиеся в помещении: дерево (мебель), бумага (документы), ПЭВМ.

Возможными источниками зажигания могут быть тепловые проявления электрической энергии (короткое замыкание. высокие сопротивления, искровые разряды статического электричества и др.).

Источниками пожара может стать неисправность или нарушение правил эксплуатации электротехнического оборудования.

Для тушения возможного пожара помещение оборудовано одним ручным порошковым огнетушителем ОП-4.

На основе ФЗ «Технический регламент о требованиях пожарной безопасности» были установлены следующие правила:

Организации, их должностные лица и граждане, нарушившие требования пожарной безопасности, несут ответственность в соответствии с законодательством Российской Федерации.

Наряду с настоящими Правилами, следует также руководствоваться иными нормативными документами по пожарной безопасности и нормативными документами, содержащими требования пожарной безопасности, утвержденными в установленном порядке.

Руководители организации и индивидуальные предприниматели на своих объектах должны иметь систему пожарной безопасности, направленную на предотвращение воздействия на людей опасных факторов пожара, в том числе их вторичных проявлений.

На каждом объекте должны быть разработаны инструкции о мерах пожарной безопасности для каждого взрывопожароопасного и пожароопасного участка (мастерской, цеха и т.п.) в соответствии с приложением данных правил.

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 в порядке, установленном руководителем.

Руководители организаций или индивидуальные предприниматели имеют право назначать лиц, которые по занимаемой должности или по характеру выполняемых работ в силу действующих нормативных правовых актов и иных актов должны выполнять соответствующие правила пожарной безопасности либо обеспечивать их соблюдение на определенных участках работ.

Для привлечения работников предприятий к работе по предупреждению и борьбе с пожарами на объектах могут создаваться пожарно-технические комиссии и добровольные пожарные формирования.

Собственники имущества, лица, уполномоченные владеть, пользоваться или распоряжаться имуществом, в том числе руководители и должностные лица организаций, лица, в установленном порядке назначенные ответственными за обеспечение пожарной безопасности, должны:

- обеспечивать своевременное выполнение требований пожарной безопасности, предписаний, постановлений и иных законных требований государственных инспекторов по пожарному надзору;

- создавать и содержать на основании утвержденных в установленном порядке норм, перечней особо важных и режимных объектов и предприятий, на которых создается пожарная охрана, органы управления и подразделения пожарной охраны, а также обеспечивать в них непрерывное несение службы и использование личного состава и пожарной техники строго по назначению.

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

Правила применения на территории организаций открытого огня, проезда транспорта, допустимость курения и проведения временных пожароопасных ра-

бот устанавливаются общеобъектовыми инструкциями о мерах пожарной безопасности.

В каждой организации распорядительным документом должен быть установлен соответствующий их пожарной опасности противопожарный режим, в том числе:

- определены и оборудованы места для курения;

- определены места и допустимое количество единовременно находящихся в помещениях сырья, полуфабрикатов и готовой продукции;

- установлен порядок уборки горючих отходов и пыли, хранения промасленной спецодежды;

- определен порядок обесточивания электрооборудования в случае пожара и по окончании рабочего дня;

- регламентированы:

- порядок проведения временных огневых и других пожароопасных работ;

- порядок осмотра и закрытия помещений после окончания работы;

- действия работников при обнаружении пожара;

- определен порядок и сроки прохождения противопожарного инструктажа и занятий по пожарно-техническому минимуму, а также назначены ответственные за их проведение.

В зданиях и сооружениях (кроме жилых домов) при единовременном нахождении на этаже более 10 человек должны быть разработаны и на видных местах вывешены планы (схемы) эвакуации людей в случае пожара, а также предусмотрена система (установка) оповещения людей о пожаре.

На объектах с массовым пребыванием людей (50 и более человек) в дополнение к схематическому плану эвакуации людей при пожаре должна быть разработана инструкция, определяющая действия персонала по обеспечению безопасной и быстрой эвакуации людей, по которой не реже одного раза в полугодие должны проводиться практические тренировки всех задействованных для эвакуации работников.

Световая, звуковая и визуальная информирующая сигнализация должна быть предусмотрена в помещениях, посещаемых данной категорией лиц, а также у каждого эвакуационного, аварийного выхода и на путях эвакуации. Световые сигналы в виде светящихся знаков должны включаться одновременно со звуковыми сигналами. Работники организаций, а также граждане должны:

- соблюдать на производстве и в быту требования пожарной безопасности, а также соблюдать и поддерживать противопожарный режим;

- выполнять меры предосторожности при пользовании газовыми приборами, предметами бытовой химии, проведении работ с легковоспламеняющимися (далее - ЛВЖ) и горючими (далее - ГЖ) жидкостями, другими опасными в пожарном отношении веществами, материалами и оборудованием;

- в случае обнаружения пожара сообщить о нем в подразделение пожарной охраны и принять возможные меры к спасению людей, имущества и ликвидации пожара.

Граждане предоставляют в порядке, установленном законодательством Российской Федерации, возможность государственным инспекторам по пожарному надзору проводить обследования и проверки принадлежащих им производственных, хозяйственных, жилых и иных помещений и строений в целях контроля за соблюдением требований пожарной безопасности.

Противопожарные системы и установки (противодымная защита, средства пожарной автоматики, системы противопожарного водоснабжения, противопожарные двери, клапаны, другие защитные устройства в противопожарных стенах и перекрытиях и т.п.) помещений, зданий и сооружений должны постоянно содержаться в исправном рабочем состоянии.

Устройства для самозакрывания дверей должны находиться в исправном состоянии. Не допускается устанавливать какие-либо приспособления, препятствующие нормальному закрыванию противопожарных или противодымных дверей (устройств).

4.8 Рекомендации по организации режима труда и отдыха пользователя.

Режимы труда и отдыха при работе с ПЭВМ и ВДТ должны организовываться в зависимости от вида и категории трудовой деятельности согласно СанПиН 2.2.2/2.4.1340-03.

По виду трудовой деятельности работу оператора можно отнести к группе «А» – работа по считыванию информации с экрана ВДТ или ПЭВМ с предварительным запросом.

Для видов трудовой деятельности устанавливается три категории тяжести и напряженности работы с ВДТ и ПЭВМ.

Для группы А категории определяются по суммарному числу считываемых знаков за рабочую смену, но не более 60 000 знаков за смену:

- 1 категория – до 20 000 знаков;
- 2 категория – до 40 000 знаков;
- 3 категория – до 60 000 знаков.

Продолжительность обеденного перерыва определяется действующим законодательством о труде и правилами внутреннего распорядка предприятия.

Для обеспечения оптимальной работоспособности и сохранения здоровья профессиональных пользователей, на протяжении рабочей смены должны устанавливаться регламентированные перерывы. Время регламентированных перерывов в течении рабочей смены следует устанавливать в зависимости от ее продолжительности, вида и категории трудовой деятельности. Продолжительность непрерывной работы без регламентированного перерыва не должна превышать двух часов. При восьмичасовой рабочей смене и работе на ВДТ и ПЭВМ регламентированные перерывы следует устанавливать:

- для 1 категории работ через 2 ч. от начала рабочей смены и через 2 ч. после обеденного перерыва продолжительностью 15 мин. каждый;

- для 2 категории работ через 2 ч. от начала рабочей смены и через 1,5–2 ч. после обеденного перерыва продолжительностью 15 мин. каждый или продолжительностью 10 мин. через каждый час работы;

- для 3 категории работ через 2 ч. от начала рабочей смены и через 1,5−2,0 ч. после обеденного перерыва продолжительностью 20 мин. каждый или продолжительностью 15 мин. через каждый час работы.

Во время регламентированных перерывов с целью снижения нервно эмоционального напряжения, утомления зрительного анализатора, устранения влияния гиподинамии и гипокинезии, предотвращения развития познотонического утомления целесообразно выполнять комплексы упражнений для глаз, для улучшения мозгового кровообращения, для снятия утомления с плечевого пояса и рук, а также общего воздействия.

В случаях возникновения у пользователя зрительного дискомфорта и других неблагоприятных субъективных ощущений, несмотря на соблюдение санитарно-гигиенических, эргономических требований, режимов труда и отдыха следует применять индивидуальный подход в ограничении времени работ с ВДТ и ПЭВМ. Коррекцию длительности перерывов для отдыха или проводить смену деятельности на другую, не связанную с использованием ВДТ и ПЭВМ.

Организационные мероприятия, устраняющие причины возникновения пожаров: обучение рабочих и служащих противопожарным правилам, проведение лекций, инструкций и т.п. Технические мероприятия: соблюдение противопожарных правил и норм при устройстве оборудования отопления, вентиляции и т.д.

Мероприятия режимного характера: запрещение курения в не установленных местах, проведения сварочных работ в пожарных помещениях. Эксплуатационные мероприятия: правильная эксплуатация машин, транспорта, оборудования и правильное содержание зданий, территорий.

4.9 Сравнение параметров рабочего места с допустимыми нормами.

Для определения соответствия условий труда требованиям нормативных документов проведем сравнительный анализ требований, установленных к рабочим

местам, оборудованным ПЭВМ и фактических параметров рабочего места. Схема размещения рабочих мест приведена на Рисунке 4. Площадь помещения 36м^2, 2 оконных проема, шириной 1,90м размещается по всей ширине торцевой северной стены кабинета. В помещении присутствует естественное и искусственное освещение (6 двойных галогеновых светильников).

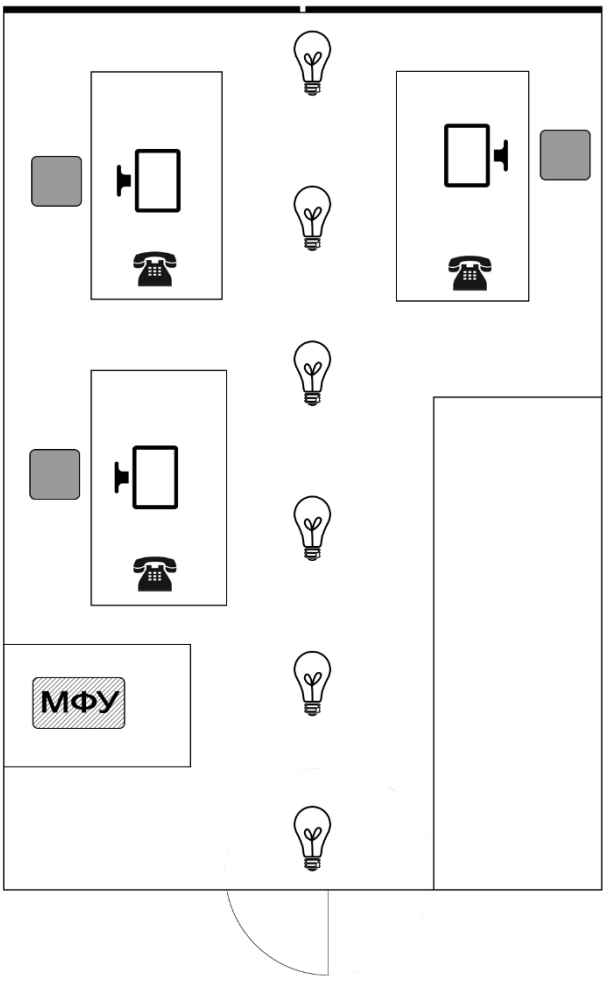

Рис. 4. Схема кабинета.

Перечень нормируемых параметров для рабочего места, сравнение их допустимых нормы и фактические значений на рабочем месте представлены в таблице 4.

Таблица 4 – Сравнение параметров рабочего места с допустимыми нормами.

Нормируемые параметры	Допустимые нормы	Фактические значения
Высота рабочей поверхности стола	от 680 до 800мм, либо 725мм	730мм
Модульные размеры рабочей поверхности стола	Ширина 800, 1000, 1200, 1400мм, глубина 800 или 1000мм	Ширина 1000мм глубина 800 мм
Ширина и глубина поверхности сиденья	Не менее 400мм	Ширина 600мм Глубина 500мм
Параметры регулировки сиденья	По характеристикам п. 4.5	Соответствуют
Площадь на одно рабочее место	не менее 4,5м2	5м2
Падение естественного света	Преимущественно слева	Для 2 рабочих мест - слева, для одного – справа.
Освещенность поверхности стола	300-500 лк	400 лк
Уровень звука	80 дБА	38 дБА
Параметры микроклимата	Температура воздуха 22-24° С Влажность воздуха 40-60%	Температура 18° С Влажность воздуха 46%

В результате проведенного анализа требований были выявлены общие требования к организации рабочих мест пользователей, требования к помещениям для работы с ПЭВМ, основные требования к освещению на рабочих местах, уровню

шума и микроклимату. На основе проведенного анализа было установлено, что условия труда на рабочем месте в основном соответствуют вышеперечисленным требованиям, за исключением температурного режима, это объясняется тем, что окна находятся на торцевой северной стене кабинета, которая является подветренной, ввиду некачественного конструктива оконных перегородок или кирпичной кладки температурный режим ниже нормы.

ЗАКЛЮЧЕНИЕ

В ходе выполнения выпускной квалификационной работы был проведен анализ информационной системы обработки информации, составляющей коммерческую тайну ФГУП «ПО «Октябрь» на основании, которого были составлены модели нарушителя и угроз информационной безопасности. Также были выявлены недостатки введенного режима коммерческой тайны, а именно отсутствие некоторой документации, которая была разработана и переработана в ходе дипломной работы, а именно:

- заявка и акт установки стороннего программного обеспечения (Приложения Б и В);
- обновление инструкции администратора по информационной безопасности (Приложение Г);
- порядок нанесения и снятия грифа «Коммерческая тайна» (Приложение Д);
- список сотрудников, допущенных к информации, составляющей коммерческую тайну (Приложение Е);
- соглашение с сотрудником о неразглашении информации, составляющей коммерческую тайну (Приложение Ж).

В результате выявленных уязвимостей в ИС ФГУП «ПО «Октябрь» приводящих к реализации той или иной угрозы, согласно составленной модели угроз и модели нарушителя безопасности, были определены обязательные мероприятия, препятствующие возникновению неблагоприятных последний от выявленных угроз, а именно:

1. От угрозы утечки видовой информации, разглашения, модификация, уничтожение информации сотрудниками, допущенными к ее обработке, предложено проведение инструктажей об ответственности и инцидентам информационной безопасности, установка RFID считывателей во входные двери в режимные подразделения и серверное помещение.

2. От угрозы установки ПО, не связанного с выполнением служебных обязанностей: предложено ограничение прав пользователей на установку стороннего программного обеспечения;

3. От угрозы утраты и модификация информации: предложено расширение дискового хранилища резервных копий путем установки дополнительных жестких дисков типа HGST HUH721212ALE604 12Tb и включение в резервное копирование ПЭВМ руководителей подразделений;

4. От сбоя системы электроснабжения рекомендуется оборудовать ключевые элементы информационной системы источниками бесперебойного питания Ippon Back Comfo Pro 1000 New.

В результате выполнения выпускной квалификационной работы проведен анализ системы, ознакомление с нормативно-правовой базой, составлен список рекомендаций по модернизации системы защиты коммерческой тайны и разработана необходимая документация для внедрения положений списка рекомендаций в систему защиты информации, составляющей коммерческую тайну предприятия.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. «Стратегия развития информационного общества в Российской Федерации» от от 07 февраля 2008 г. № Пр-2012 [Электронный ресурс]. – Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_92004/, свободный. – Загл. с экрана.;

2. ГОСТ 12.1.004–91 ССБТ «Пожарная безопасность. Общие требования» [Электронный ресурс]. – Режим доступа : http://docs.cntd.ru/document/9051953, свободный. – Загл. с экрана.;

3. Конституция Российской Федерации [Электронный ресурс]. – Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_28399/, свободный. – Загл. с экрана.;

4. Руководящий документ ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. – Режим доступа : http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-fstek-rossii-2008-god, свободный. – Загл. с экрана.;

5. СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы» [Электронный ресурс]. – Режим доступа : https://rg.ru/2003/06/21/134.html, свободный. – Загл. с экрана.;

6. СанПиН 2.2.4.3359-16 «Санитарно-эпидемиологические требования к физическим факторам на рабочих местах» [Электронный ресурс]. – Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_203183/, свободный. – Загл. с экрана.;

7. Федеральный закон от 22 августа 2008 г. № 123-ФЗ «Технический регламент о требованиях пожарной безопасности» [Электронный ресурс]. – Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_78699/, свободный. – Загл. с экрана.;

8. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. – Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61801/, свободный. – Загл. с экрана.;

9. ФСТЭК России от 15 февраля 2008 г. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. – Режим доступа: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379, свободный. – Загл. с экрана.

10. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/, свободный. – Загл. с экрана.;

11. Куприянов, А. И. Основы защиты информации: учебное пособие/ А.И. Куприянов. – М.: Академия, 2007. – 254 с;

12. Северин, В. А. Коммерческая тайна в России/ В.А. Северин. – М.: Зерцало-М, 2009. – 466 с;

ПРИЛОЖЕНИЕ А

Модель угроз информационной безопасности коммерческой тайны ФГУП «ПО «Октябрь».

1. Общие положения.

Данная модель угроз безопасности информации, составляющей коммерческую тайну ФГУП «ПО «Октябрь», разработана на основании:

- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. приказом ФСТЭК России от 15.02.2008 г.);

- «Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. Приказом ФСТЭК России 14.02.2008 г.).

Модель угроз описывает уровень исходной защищенности информационной системы, в которой производится обработка информации, составляющей коммерческую тайну, описание угроз информационной безопасности и определяет актуальные угрозы.

2. Определение уровня исходной защищенности.

Определение уровня исходной защищенности описано в таблице А.1.

Таблица А.1. Уровень исходной защищенности.

Технические и эксплуатационные характеристики системы	Уровень защищенности		
	высокий	средний	низкий
1. По территориальному размещению:			
система, развернутая в пределах контролируемой зоны периметра предприятия			+
2. По наличию соединения с сетями общего пользования:			
система имеет обособленные ПЭВМ, имеющие выход в сеть общего пользования, не связанные с ЛВС предприятия		+	

3. По встроенным операциям со сведениями и разграничению прав доступа:			
чтение, передача для всех данных, модификация и удаление только для данных своего подразделения		+	
4. По несанкционированному доступу в систему или помещения:			
доступ в систему предоставляется только зарегистрированным пользователям, доступ в помещения только по электронным пропускам	+		
5. По контролю выноса готовой продукции:			
сотрудниками отдела безопасности во внеплановом и случайном порядке производится осмотр (в том числе с использованием ручного металлоискателя) личных вещей сотрудников в конце рабочего дня на выходных турникетах		+	
Характеристики системы защиты	20%	60%	20%

Таким образом, система имеет средний (Y_1=5) уровень исходной защищенности, т.к. более 75% характеристик соответствуют уровню защищенности не ниже «среднего».

3. Определение актуальных угроз безопасности информации, составляющей коммерческую тайну.

Определение вероятности реализации угроз безопасности системы обработки информации, составляющей коммерческую тайну представлено в таблице А.2.

Таблица А.2. Модель угроз безопасности системы обработки информации, составляющей коммерческую тайну.

Тип угроз безопасности	Анализ угроз	Вероятность реализации (Y_2)	Коэффициент реализуемости угрозы (Y)	Возможность реализации
1. Угрозы утечки по техническим каналам				
1.1 Угрозы утечки акустической информации	В системе отсутствует голосовое управление средствами обработки конфиденциальных сведений	Маловероятна (0)	0,25	Низкая

1.2 Угрозы утечки видовой информации	Проход в подразделения, в которых ведется обработка конфиденциальных сведений организован по электронным пропускам. Лицам иных подразделений в случае производственной необходимости разрешен проход в эти помещения в сопровождении уполномоченных сотрудников (этого подразделения).	Средняя (5)	0,5	Средняя
1.3 Угрозы утечки по каналам ПЭМИН	Имеются ВТСС и линии связи, выходящие за пределы помещений подразделений. А также линии связи, выходящие за пределы контролируемой зоны.	Средняя (5)	0,35	Средняя
1. Угрозы несанкционированного доступа к информации				
2.1 Угрозы уничтожения, хищения аппаратных средств, носителей информации путем физического доступа к элементам (АРМ)				
2.1.1 Кража ПЭВМ	Вынос ПЭВМ разрешен только техническим специалистом в сопровождении соответствующей документации.	Маловероятна (0)	0,25	Низкая
2.1.2 Кража носителей информации	Доступ в помещения, в которых ведется обработка конфиденциальных сведений, ограничен организационными мерами.	Маловероятна (0)	0,5	Низкая
2.1.3 Кража атрибутов доступа, информации.	Доступ в помещения, в которых ведется обработка конфиденциальных сведений, ограничен организационными мерами. Доступ к информационным ресурсам в ЛВС предприятия ограничен логином и паролем ранее зарегистрированных пользователей.	Маловероятна (0)	0,25	Низкая
2.1.4 Несанкционированный доступ к информации при техническом обслуживании узлов ПЭВМ.	Техническое обслуживание осуществляется сотрудниками предприятия. При необходимости передачи в сторонние организации с целью обслуживания, жесткие диски не передаются.	Маловероятна (0)	0,25	Низкая
2.2 Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств.				

2.2.1 Действия вредоносных программ (вирусов)	На АРМ установлено антивирусное ПО «Dr.Web». Пользователям запрещено производить отключение системы антивирусной защиты. Обновление баз выполняется регулярно через ЛВС предприятия.	Маловероятна (0)	0,25	Низкая
2.2.2 Установка ПО, не связанного с исполнением служебных обязанностей	Введено разграничение прав пользователей на установку ПО. Пользователи проинструктированы о политике установки ПО.	Средняя (5)	0,5	Средняя
2.3 Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования системы обработки конфиденциальной информации из-за сбоев в ПО, а также угроз не антропогенного и стихийного характера.				
2.3.1 Утрата атрибутов доступа	Доступ к информационным ресурсам в ЛВС предприятия ограничен логином и паролем ранее зарегистрированных пользователей. Пользователи проинструктированы о порядке действий в случае утраты или компрометации паролей.	Низкая (2)	0,35	Низкая
2.3.2 Непреднамеренная модификация, уничтожение информации сотрудниками	Резервное копирование осуществляется раз в 2 недели.	Средняя (5)	0,5	Средняя
2.3.3 Сбой системы электроснабжения	Отсутствуют источники бесперебойного питания для каждого ключевого элемента.	Средняя (5)	0,5	Средняя
2.3.4 Стихийное бедствие	План восстановления работы системы после сбоев регламентирован в нормативных документах.	Низкая (2)	0,35	Низкая
2.4 Угрозы преднамеренных действий внутренних нарушителей				
2.4.1 Доступ лиц к модификации, уничтожению информации, не допущенных к ее обработке	Доступ в помещения, в которых ведется обработка конфиденциальных сведений, ограничен организационными мерами.	Низкая (2)	0,35	Низкая
2.4.2 Разглашение, модификация, уничтожение информации сотрудниками, допущенными к ее обработке	Сотрудники, допущенные к обработке сведений конфиденциального характера, ознакомлены о порядке работы и подписали Договор о неразглашении.	Средняя (5)	0,5	Средняя

Опасность угроз определяется по методическим в документе «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. приказом ФСТЭК России от 15.02.2008 г.). Оценка опасности угроз представлена в таблице 3.

Таблица А.3. Оценка опасности угроз.

Тип угроз безопасности	Опасность угрозы
1.1 Угрозы утечки акустической информации	Низкая
1.2 Угрозы утечки видовой информации	Средняя
1.3 Угрозы утечки по каналам ПЭМИН	Низкая
2.1.1 Кража ПЭВМ	Низкая
2.1.2 Кража носителей информации	Низкая
2.1.3 Кража атрибутов доступа, информации.	Низкая
2.1.4 Несанкционированный доступ к информации при техническом обслуживании узлов ПЭВМ.	Низкая
2.2.1 Действия вредоносных программ (вирусов)	Низкая
2.2.2 Установка ПО, не связанного с исполнением служебных обязанностей	Средняя
2.3.1 Утрата атрибутов доступа	Низкая
2.3.2 Непреднамеренная модификация, уничтожение информации сотрудниками	Средняя
2.3.3 Сбой системы электроснабжения	Средняя
2.3.4 Стихийное бедствие	Низкая
2.4.1 Доступ лиц к модификации, уничтожению информации, не допущенных к ее обработке	Низкая
2.4.2 Разглашение, модификация, уничтожение информации сотрудниками, допущенными к ее обработке	Средняя

Для определения угрозы как “актуальной”, уровни ее опасности и возможности реализации, должны быть не ниже “среднего”. Определение актуальности угрозы представлено в таблице А.4.

Таблица А.4. Определение актуальности угрозы.

Показатель опасности угрозы / Возможность реализации угрозы	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	неактуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	неактуальная	актуальная	актуальная

Параметр актуальности рассмотренных угроз представлен в таблице А.5.

Таблица А.5. Актуальность угроз

Тип угроз безопасности	Актуальность угрозы
1	2
1.1. Угрозы утечки акустической информации	Неактуальная
1.2. Угрозы утечки видовой информации	Актуальная
1.3. Угрозы утечки по каналам ПЭМИН	Неактуальная
2.1.1. Кража ПЭВМ	Неактуальная
2.1.2. Кража носителей информации	Неактуальная
2.1.3. Кража атрибутов доступа, информации.	Неактуальная
2.1.4. Несанкционированный доступ к информации при техническом обслуживании узлов ПЭВМ.	Неактуальная
2.2.1. Действия вредоносных программ (вирусов)	Неактуальная
2.2.2. Установка ПО, не связанного с исполнением служебных обязанностей	Актуальная

2.3.1. Утрата атрибутов доступа	Неактуальная
2.3.2. Непреднамеренная модификация, уничтожение информации сотрудниками	Актуальная
2.3.3. Сбой системы электроснабжения	Актуальная
2.3.4. Стихийное бедствие	Неактуальная
2.4.1. Доступ лиц к модификации, уничтожению информации, не допущенных к ее обработке	Неактуальная
2.4.2. Разглашение, модификация, уничтожение информации сотрудниками, допущенными к ее обработке	Актуальная

ПРИЛОЖЕНИЕ Б

ЗАЯВКА НА УСТАНОВКУ СТОРОННЕГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

УТВЕРЖДАЮ

Ф.И.О. _____

должность _____

Приказ № ___ от «___» _____ 201__ г.

_____

инвентарный номер ПЭВМ

_____

расположение ПЭВМ

_____

описание программного обеспечения

_____

обоснование заявки

_____

особые отметки

_____

контактный телефон подразделения

Сотрудник подразделения: _____ _____ _____

подпись дата фамилия

СОГЛАСОВАНО:

Начальник отдела ПД ИТР, ТЗИ и СЭ: _____ _____ _____

подпись дата фамилия

ПРИЛОЖЕНИЕ В

АКТ УСТАНОВКИ СТОРОННЕГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

УТВЕРЖДАЮ

Ф.И.О. _____

должность _____

Приказ № ___ от «___» _____ 201__ г.

_____

инвентарный номер ПЭВМ

_____

расположение ПЭВМ

_____

описание программного обеспечения

_____

контактный телефон подразделения

Программное обеспечение установил и подготовил к использованию:

Администратор безопасности сети: _____ _____ _____

подпись дата фамилия

СОГЛАСОВАНО:

Начальник отдела ПД ИТР, ТЗИ и СЭ: _____ _____ _____

подпись дата фамилия

ПРИЛОЖЕНИЕ Г

Инструкция Администратора по информационной безопасности отдела ТЗИ и СЭ ФГУП ПО «Октябрь».

1. Общие положения

1.1. Настоящая инструкция определяет функциональные обязанности, права и ответственность Администратора по информационной безопасности отдела технической защиты информации и спецэкспертиз ФГУП ПО «Октябрь»

1.2. Администратор назначается и освобождается от должности в установленном действующим трудовым законодательством порядке.

1.3. Администратор должен знать:

- законодательные и нормативные правовые акты о государственной (служебной, коммерческой) тайне;
- постановления, распоряжения, приказы, методические и нормативные материалы по вопросам, связанным с обеспечением технической защиты информации;
- особенности деятельности и порядок прохождения служебной информации;
- систему организации комплексной защиты информации;
- методы и средства получения, обработки и передачи информации;
- научно-техническую и другую специальную литературу по техническому обеспечению защиты информации;
- технические средства защиты информации;
- программно-математические средства защиты информации;
- порядок оформления технической документации по защите информации;
- каналы возможной утечки информации;
- методы анализа и защиты информации;
- организацию работ по защите информации;
- инструкции по соблюдению режима проведения специальных работ;
- отечественный и зарубежный опыт в области технической разведки и защиты информации.

2. Функциональные обязанности

2.1. Администратор:

2.1.1. Выполняет работу по проектированию и внедрению специальных технических и программно-математических средств защиты информации, обеспечению организационных и инженерно-технических мер защиты информационных систем, проводит исследования с целью нахождения выбора наиболее целесообразных практических решений в пределах поставленной задачи.

2.1.2. Осуществляет подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по техническим средствам и способам защиты информации.

2.1.3. Участвует в рассмотрении проектов технических заданий, планов и графиков проведения работ по технической защите информации, в разработке необходимой технической документации.

2.1.4. Осуществляет методики расчетов и программы экспериментальных исследований по технической защите информации, выполняет расчеты в соответствии с разработанными методиками и программами.

2.1.5. Проводит сопоставительный анализ данных исследований и испытаний, изучает возможные источники и каналы утечки информации.

2.1.6. Осуществляет разработку технического обеспечения системы защиты информации, технического обслуживания средств защиты информации, принимает участие в составлении рекомендаций и предложений по совершенствованию и повышению эффективности защиты информации, в написании и оформлении разделов научно-технических отчетов.

2.1.7. Участвует в проведении аттестации объектов информатизации, технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации по соответствующим классам безопасности.

2.1.8. Проводит контрольные проверки работоспособности и эффективности действующих систем и технических средств защиты информации, составляет и оформляет акты контрольных проверок, анализирует результаты проверок и разрабатывает предложения по совершенствованию и повышению эффективности принимаемых мер.

2.1.9. Изучает и обобщает опыт работы других учреждений, организаций и предприятий по использованию технических средств и способов защиты информации с целью повышения эффективности и совершенствования работ по ее защите и сохранению государственной тайны.

2.1.10. Выполняет работы в установленные сроки на высоком научно-техническом уровне, соблюдая требования инструкций по режиму проведения работ.

3. Периодичность выполнения работ.

3.1. Администратор проводит:

- проверку журнала регистрации попыток нарушения системы защиты информации и несанкционированного доступа к ней не реже 1 раза в месяц;
- периодическое тестирование средств защиты информации не реже 1 раза в год;
- обновление антивирусных баз и проверку наличия вирусов на защищаемом объекте не реже 1 раза в месяц.

4. Права

4.1. Администратор имеет право:

4.1.1. запрашивать и получать необходимые материалы и документы, относящиеся к вопросам деятельности по защите информации;

4.1.2. вступать во взаимоотношения с подразделениями сторонних учреждений и организаций для решения оперативных вопросов производственной деятельности, входящей в компетенцию Администратора;

4.1.3. создавать, удалять учетные записи пользователей в соответствии с организационно-распорядительной документацией (служебные записки, приказы, распоряжения);

4.1.4. менять состав прикладного программного обеспечения на основании организационно-распорядительной документации (служебные записки, приказы, распоряжения), предварительно согласовав с органом по аттестации объектов информатизации (уведомление, письмо);

4.1.5. в случае сбоя в работе ПЭВМ переустанавливать СЗИ от НСД, ОС или ПО;

4.1.6. в случае выхода из строя СВТ обратиться в орган по аттестации объектов информатизации для согласования дальнейших действий;

4.1.7. вносить изменения в аттестационную документацию после выполнения каких-либо работ, перечисленных в пунктах 4.1.3 – 4.1.6.

5. Ответственность

5.1. Администратор несет ответственность за:

5.1.1. Невыполнение своих функциональных обязанностей.

5.1.2. Недостоверную информацию о состоянии выполнения полученных заданий и поручений, нарушение сроков их исполнения.

5.1.3. Нарушение Правил внутреннего трудового распорядка, правил противопожарной безопасности и техники безопасности, установленных в отделе ТЗИ и СЭ ФГУП ПО «Октябрь»

6. Условия работы

6.1. Режим работы Администратора определяется в соответствии с Правилами внутреннего трудового распорядка, установленными в отделе ТЗИ и СЭ ФГУП ПО «Октябрь»;

6.2. В связи с производственной необходимостью Администратор может направляться в командировки.

ПРИЛОЖЕНИЕ Д

Порядок установления и снятия грифа «Коммерческая тайна».

Настоящий порядок установления и снятия грифа «Коммерческая тайна» предусматривает:

- кто, когда и как устанавливает гриф «Коммерческая тайна» документу (изделию);

- кто, когда и как снимает гриф «Коммерческая тайна» с документа (изделия);

- права, обязанности и ответственность должностных лиц, устанавливающих и снимающих ограничительный гриф;

- контроль за этой сферой деятельности.

1. Установление грифа «Коммерческая тайна» документам и изделиям

Гриф «Коммерческая тайна» устанавливается документу (изделию) разработчиком этого документа (изделия) на стадии подготовки проекта документа и технической документации на изделие.

При установлении грифа «Коммерческая тайна» разработчик руководствуется требованиями заказчика и Перечнем сведений, составляющих коммерческую тайну ФГУП “ПО “Октябрь”. Сведения, которые должны являться коммерческой тайной, заказчику целесообразно указывать в договоре на проведение этих работ.

Требования заказчика в части сведений, являющихся коммерческой тайной, и Перечень сведений, составляющих коммерческую тайну предприятия-исполнителя в части выполняемой работы, не должны противоречить друг другу. Сведения, составляющие коммерческую тайну, могут быть указаны в других документах (ТЗ, ТТЗ), но с соответствующей ссылкой на это обстоятельство в договоре.

На документах гриф «Коммерческая тайна» проставляется на первом (титульном) листе и на обложке в правом углу в соответствии с ГОСТ 6.39-90. На чертежно-конструкторской и технологической документации гриф проставляется в местах, отведенных соответствующими ГОСТами.

Гриф «Коммерческая тайна» установленный изделию, указывается в сопроводительной документации на изделие (в формуляре, паспорте). При этом в сопроводительной документации указывается, какая составная часть изделия содержит охраняемые сведения.

Гриф «Коммерческая тайна» проставляется на сопроводительном письме, если документы, имеющие гриф «Коммерческая тайна» сопровождаются вместе с ним.

Предприятие-получатель имеет право установить полученным документам (изделиям) гриф «Коммерческая тайна» в соответствии со своим «Перечнем сведений, составляющих коммерческую тайну» в случаях, если:

- предприятие-разработчик документа (изделия) было обязано установить гриф «Коммерческая тайна» по условиям договора. Предприятие-разработчик документа (изделия) немедленно уведомляется о допущенном им нарушении договора. Если предприятие, допустившее нарушение, смогло своевременно реализовать необходимые и достаточные меры по защите охраняемой информации от утечки, то инцидент может быть исчерпан. В противном случае вопрос о возмещении ущерба решается в соответствии с действующим законодательством;

- предприятие-разработчик документа (изделия) не связано с предприятием-получателем условиями договора, но по договоренности с предприятием-получателем согласно включить эти сведения в свой «Перечень сведений, составляющих коммерческую тайну» и обеспечить необходимую защиту этой информации. Следует иметь в виду, что без согласия предприятия-разработчика и принятия им соответствующих мер установление грифа «Коммерческая тайна» предприятием-получателем документа (изделия) лишено смысла.

При необходимости, можно вводить ограничительные пометки психологического характера. Например, на определенные категории документов, содержащих охраняемые сведения, можно прикреплять ярко выполненные таблички: «На столе не оставлять», «Хранить в сейфе».

2. Снятие грифа «Коммерческая тайна» с документов и изделий

Снятие грифа «Коммерческая тайна» с документа или изделия осуществляет должностное лицо, подписавшее (утвердившее) этот документ или техническую документацию на изделие, или руководитель предприятия.

Основанием для снятия грифа «Коммерческая тайна» с документов и изделий являются:

- требования заказчика;

- соответствующая корректировка «Перечня сведений, составляющих коммерческую тайну» предприятия;

- гриф «Коммерческая тайна» был установлен неправильно;

- истечение установленного срока действия грифа.

О снятии грифа «Коммерческая тайна» соответствующее должностное лицо делает отметку на самом документе и в технической (сопроводительной) документации на изделие путем зачеркивания грифа с проставлением своей подписи и даты.

Лица, осуществляющие учет документов (изделий) с грифом «Коммерческая тайна», делают необходимые отметки в соответствующих учетных документах (формах) с указанием фамилии лица, снявшего гриф, и даты снятия.

О снятии грифа «Коммерческая тайна» предприятие, устанавливавшее гриф, извещает все предприятия, связанные договорными обязательствами с предприятием-разработчиком в части охраны коммерческой тайны. Извещение является основанием для снятия грифа «Коммерческая тайна» с полученных документов или изделий. Выполняют эту операцию лица, осуществляющие учет документов или изделий с грифом «Коммерческая тайна».

3. Обеспечение правильности определения своевременности установления и снятия грифа «Коммерческая тайна»

Ответственность за правильность определения и своевременность установления и снятия грифа «Коммерческая тайна» несут разработчики этих документов или изделий и руководители, подписавшие (утвердившие) документы или техническую документацию на изделия.

Контроль за правильностью определения и своевременностью установления и снятия грифа «Коммерческая тайна» осуществляют лица, назначенные руководителем предприятия.

ПРИЛОЖЕНИЕ Е

Список сотрудников ФГУП «ПО «Октябрь», имеющих доступ к информации, составляющей коммерческую тайну.

УТВЕРЖДАЮ

Ф.И.О. _____

должность _____

Приказ № ___ от « ___ » _____ 201__ г.

Ф.И.О. сотрудника	Должность	Объем представленной информации, составляющей коммерческую тайну
Иванов Иван Иванович	Ведущий инженер отдела 130	Перечень информации, составляющей коммерческую тайну, с которой сотрудник ознакомлен.
Калинина Анжела Васильевна	Бухгалтер	Перечень информации, составляющей коммерческую тайну, с которой сотрудник ознакомлен.

_____ _____

подпись расшифровка

ПРИЛОЖЕНИЕ Ж

Соглашение № ___

о неразглашении информации, составляющей коммерческую тайну

ФГУП «ПО «Октябрь»

Я, _____

ФИО должность работника

добровольно принимаю на себя следующие обязательства:

1. Выполнять установленный ФГУП «ПО «Октябрь» режим коммерческой тайны.
2. Не разглашать информацию, составляющую коммерческую тайну, обладателями которой являются ФГУП «ПО «Октябрь» и без их согласия не использовать эту информацию в личных целях.
3. Передать ФГУП «ПО «Октябрь» при прекращении или расторжении трудового договора, имеющиеся в пользовании работника материальные носители информации, содержащие информацию, составляющую коммерческую тайну.
4. Письменно информировать непосредственного руководителя ФГУП «ПО «Октябрь» о следующих фактах:
   - о попытках получить от меня информацию, составляющую коммерческую тайну;
   - о попытках других работников ФГУП «ПО «Октябрь» воспользоваться мобильными компьютерами, личными фотоаппаратами, съемными носителями информации на рабочем месте;
   - о любых иных действиях работников компании и иных лиц, представляющих угрозу для соблюдения режима коммерческой тайны.
5. Не разглашать и не передавать третьим лицам информацию, составляющую коммерческую тайну после прекращения трудовых отношений с ФГУП «ПО «Октябрь».
6. Выполнять требования нормативных правовых актов и локальных правовых актов, регламентирующих вопросы защиты конфиденциальной информации.

_____

(Подпись работника)

Окончание Приложения Е

СВЕДЕНИЯ ОБ ОЗНАКОМЛЕНИИ РАБОТНИКА С РЕЖИМОМ КОММЕРЧЕСКОЙ ТАЙНЫ ФГУП «ПО «ОКТЯБРЬ» И ПЕРЕЧНЕМ ИНФОРМАЦИИ, СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ ФГУП «ПО «ОКТЯБРЬ»

Я выражаю свое согласие на получение доступа к информации, составляющей коммерческую тайну.

Я ознакомлен с Положением о коммерческой тайне ФГУП «ПО «Октябрь», Режимом коммерческой тайны, Перечнем информации, составляющей коммерческую тайну, Приказом об установлении на ФГУП «ПО «Октябрь» режима коммерческой тайны.

Я предупрежден (а), что в случае нарушения режима коммерческой тайны могу быть привлечен (а) к следующим видам ответственности:

уголовной ответственности в виде штрафа в размере до ста двадцати тысяч рублей либо лишением свободы на срок до трех лет (ст. 183 УК РФ)

дисциплинарной ответственности в виде увольнения (пп. «в» п. 6 ст. 81 ТК РФ)

полной материальной ответственности в виде полного возмещения причиненного ущерба (п. 7 ст. 243 ТК РФ)

гражданско-правовой ответственности в виде возмещения убытков (ст. 15, ст. 1472 ГК РФ)

_____

(Подпись работника)