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»

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

Разработка защищенной информационной системы персональных данных ООО «Трехгорный керамический завод»

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ – 10.03.01.2018.182.ПЗ ВКР

Руководитель проекта,
Ген. директор ООО «Диджитер»
_____ С.А. Сабельников
_____ 2018 г.

Автор проекта,
студент группы КЭ-471
_____ Е.В. Горбатова
_____ 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 10.03.01 «Информационная безопасность»

УТВЕРЖДАЮ

Заведующий кафедрой

_____ А.Н. Соколов

_____ 2018 г.

З А Д А Н И Е

на выпускную квалификационную работу студента

Горбатовой Елизаветы Владимировны

Группа *КЭ-471*

1 Тема работы

Разработка защищенной информационной системы персональных данных

ООО "Трехгорный керамический завод"

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

2 Срок сдачи студентом законченной работы *27.05.2018*

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)

Провести обследование ООО «Трехгорный керамический завод»;

Составить технический паспорт ИСПДн «Сотрудники» ООО «Трехгорный керамический завод»;

Установить перечень персональных данных, подлежащих защите в ИСПДн «Сотрудники»;

Разработать техническое задание на создание системы защиты персональных данных на предприятии ООО «Трехгорный керамический завод»;

Разработать частную модель угроз информационной безопасности ООО «Трехгорный керамический завод»;

Провести теоретическое обоснование выбора средств защиты;

Разработать проект создания системы защиты на предприятии ООО «Трехгорный керамический завод»;

Рассчитать бюджет проекта создания системы защиты на предприятии ООО «Трехгорный керамический завод».

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

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)

7 Дата выдачи задания _____*25 января 2018*_____

Руководитель,
Ген. директор ООО «Диджитер» _____ С.А. Сабельников

Задание принял к исполнению _____ Е.В. Горбатова

КАЛЕНДАРНЫЙ ПЛАН

Наименование этапов выпускной квалификационной работы (проекта)	**Срок выполнения этапов работы**	**Отметки о выполнении руководителя**
Введение	*24.03.2018*	
Анализ состояния защиты информации в ООО «Трехгорный керамический завод»	*24.03.2018*	
Теоретическое обоснование выбора средств защиты	*30.04.2018*	
Разработка проекта создания системы защиты на предприятии ООО «Трехгорный керамический завод»	*30.04.2018*	
Заключение	*30.04.2018*	
Библиографический список	*30.04.2018*	
Предзащита ВКР	*04.06.2018*	
Защита ВКР	*11.06.2018*	

Заведующий кафедрой _____ А.Н. Соколов

Руководитель работы _____ С.А. Сабельников

Студент _____ Е.В. Горбатова

АННОТАЦИЯ

Горбатова Е.В. Разработка защищенной информационной системы персональных данных ООО "Трехгорный керамический завод"– Челябинск: ЮУрГУ, КЭ-471, 129 с., 3 ил., 14 табл., библиогр. список – 23 наим., 12 прил.

Выпускная квалификационная работа выполнена с целью создания системы защиты персональных данных в ООО "Трехгорный керамический завод".

В выпускной квалификационной работе отражены все этапы создания системы защиты персональных данных, от сбора исходных данных до заключения о соответствии нормативным документам РФ по защите персональных данных.

В процессе выполнения квалификационной работы было проведено предпроектное обследование предприятия, созданы все необходимые документы, регламентирующие порядок защиты информации, а также описывающие информационную систему персональных данных предприятия. Было проведено проектирование системы защиты, включающее в себя выбор средств защиты, предотвращающих актуальные угрозы предприятия, обоснования их эффективности и экономической целесообразности.

ОГЛАВЛЕНИЕ

СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ

АПКШ – аппаратно-программный комплекс шифрования;
АРМ – автоматизированное рабочие место;
АС – автоматизированная система;
ВТСС – вспомогательные технические средства и системы;
ЗИ – защита информации;
ИБ – информационная безопасность;
ИС – информационная система;
ИСПДн – информационная система персональных данных;
ИТ – информационные технологии;
МСЭ – межсетевой экран;
НСД – несанкционированный доступ;
ООО – Общество с ограниченной ответственностью;
ОТСС – основные технические средства и системы;
ПАК – программно-аппаратный комплекс;
ПДн – персональные данные;
ПО – программное обеспечение;
РД – руководящие документы;
РФ – Российская Федерация;
СВТ – средства вычислительной техники;
ФЗ – Федеральный закон;
ФСБ – Федеральная служба безопасности;
ФСТЭК – Федеральная служба по техническому и экспортному контролю.

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций [1].

Базовые угрозы информационной безопасности – нарушение конфиденциальности, нарушение целостности и отказ в обслуживании [1].

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 [1].

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение),

извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных [7].

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) [7].

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы [1].

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем [1].

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа [1].

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных [1].

Уязвимость – некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации [1].

ВВЕДЕНИЕ

В настоящее время Россия является активным участником международного информационного обмена, что сделало задачу защиты частной жизни граждан особенно актуальной. Правовой режим защиты персональных данных работника в современных условиях приобретает актуальное значение в виду того, что российским законодательством, и, прежде всего Конституцией РФ провозглашен принцип невмешательства в частную жизнь лица, который предполагает предоставление каждому члену общества гарантированной государством возможности контролировать сбор и обработку информации о его частной жизни.

Продукцией, выпускаемой на предприятии, является пропант алюмосиликатный (керамический) средней прочности. Керамический пропант имеет огромное значение в процессе добычи нефти. Это изобретение было создано для увеличения нефтеотдачи пластов при проведении операции ГРП, пропант предотвращает смыкание трещины разрыва, обеспечивая свободный проход нефтегазонасыщенного конденсата к устью скважины.

В процессе создания продукции участвуют более 500 человек, и в соответствии с Федеральным законом № 152-ФЗ предприятие должно обеспечить защиту персональных данных всех этих людей – своих сотрудников и принять все необходимые меры по защите их ПДн.

Таким образом, актуальность данной работы обусловлена необходимостью создания защиты автоматизированной системы обработки персональных данных в ООО «Трехгорный керамический завод».

Объектом выпускной квалификационной работы является ООО «Трехгорный керамический завод».

Предметом выпускной квалификационной работы является автоматизированная система обработки персональных данных в данной организации.

Целью дипломной работы является выбор и обоснование мер по защите автоматизированной системы обработки персональных данных.

В соответствии с поставленной целью необходимо решить следующие задачи:

1. Провести анализ информационной системы ООО «Трехгорный керамический завод» и обосновать необходимость создания системы защиты персональных данных.
2. Проанализировать и теоретически обосновать выбор средств защиты информации.
3. Разработать проект по созданию системы защиты персональных данных в ООО «Трехгорный керамический завод».

1. АНАЛИЗ СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В ООО «ТРЕХГОРНЫЙ КЕРАМИЧЕСКИЙ ЗАВОД» И СУЩЕСТВУЮЩИЕ ПРОБЛЕМЫ

1.1. Разработка технического паспорта

Для создания системы защиты информации было проведено предпроектное обследование предприятия, в результате которого был составлен технический паспорт (Приложение А).

В техническом паспорте приведен состав ОТСС, ВТСС, схемы их размещения, перечень установленных средств защиты информации и программного обеспечения.

В качестве объекта защиты была выбрана ИСПДн «Сотрудники» ООО «Трехгорный керамический завод».

1.2. Разработка модели деятельности

В ходе обследования работы ИСПДн «Сотрудники» была построена модель деятельности (Приложение Л). В этой схеме отражаются основные этапы технологического процесса обработки защищаемой информации от подготовки к обработке информации ограниченного доступа до сохранения результатов.

Данная модель необходима для выявления потоков информации ограниченного доступа.

1.3. Выявление защищаемой информации

В результате проведенного предпроектного обследования, ознакомления с информацией ограниченного доступа и организационно-распорядительной документацией, была выявлена следующая защищаемая информация: перечень персональных данных, подлежащих защите в автоматизированной системе обработки персональных данных «Сотрудники».

Перечень персональных данных, обрабатываемых в организации, представлен в приложении. (Приложение В).

1.4. Описание информационной системы

Система защиты информации в АС «Сотрудники» ООО «Трехгорный керамический завод» основана на использовании организационных, правовых и программно-аппаратных мер.

Организационные меры включают в себя инструкции администратора, инструкции пользователей, инструкцию по эксплуатации СЗИ, инструкцию по антивирусной защите, инструкцию по парольной защите, инструкцию по резервированию, журнал учета машинных носителей.

В рамках ВКР была разработана инструкция по антивирусной защите (Приложение Г), инструкция администратора (Приложение Е), инструкция пользователя (Приложение Ж), инструкция по эксплуатации СЗИ (Приложение З), инструкция по парольной защите (Приложение Д), журнал учета машинных носителей (Приложение И), приказы о назначении ответственного за организацию обработки ПДн и ответственного за обеспечение ИБ (Приложение М). Инструкция по резервированию и журнал учета лиц ранее существовали на предприятии.

Правовые меры включают в себя нормативно-правовые документы, регулирующие деятельность организации в области обеспечения защиты информации:

– Трудовой кодекс Российской Федерации [13].

– Гражданский кодекс Российской Федерации [4].

– Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» [8].

– Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных» [7].

– Приказ ФСТЭК России N 21 от 18 февраля 2013 г. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн» [9].

– Постановление Правительства РФ от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [15].

– Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» [8].

Программно-аппаратные меры включают в себя комплекс программно-аппаратных средств, обеспечивающих работу автоматизированной системы и ее защиту. В рамках ВКР была проведена инвентаризация автоматизированной системы, результаты которой представлены в Таблицах 1, 2 и 3.

Таблица 1 – Программное обеспечение

Наименование	Версия
Microsoft Windows 7 Professional	6.1.7601.17514
1С.Кадры	6.7.2
Microsoft office 2007	12.0.6425.1000
Spu_orb	
AVG AntiVirus FREE	17.9.3040

Таблица 2 – Список ОТСС

№ п/п	Название АРМ	Вид оборудования	Модель	Инвентарный (заводской) номер	Расположение
1.	АРМ Афанасьева	Системный блок	Microlab	FGH3457788HJIH	Кабинет отдела кадров
		Монитор	Aser	GHFTG4568JFF	
		Клавиатура	Logitech	TDE45678999JHG	
		Мышь	Smartbuy	REWD341178JKLK	
		Принтер	HP LaserJet P2055	FHFTHG428FGJ	
2.	АРМ Лапина	Системный блок	Microlab	FLWYO5867BHF	Кабинет отдела кадров
		Монитор	Aser	FOPPQW30905G	
		Клавиатура	Logitech	AWRG567KNG	
		Мышь	Aquarius	FH56333GHYOI	
		МФУ	Canon	DGRDHG56754G	

Таблица 3 – Список ВТСС

№ п/п	Вид оборудования	Модель	Инвентарный (заводской) номер	Расположение
1	Телефонный аппарат	Panasonic	GJDH233J	Кабинет отдела кадров
2	Телефонный аппарат	Panasonic	ETF3473FG	
3	Коммутатор	D-Link	EKRS453G	
4	Датчик пожарной сигнализации	-	-	
5	Датчик пожарной сигнализации	-	-	

1.5. Выявление объектов защиты

На основе перечня защищаемой информации, изучения модели деятельности и технологического процесса обработки информации были выявлены объекты защиты и составлен их перечень:

– два автоматизированных рабочих места, на которых обрабатывается защищаемая информация;

– средства ввода-вывода и отображения информации;

– система бесперебойного питания АРМ;

– линии и средства связи, системы обеспечения функционирования СВТ и деятельности организации;

– бумажные и электронные носители информации;

– персонал.

Более подробно перечень объектов защиты представлен в Приложении А.

1.6. Разработка модели угроз и уязвимостей для важных объектов защиты

Модель угроз безопасности информации, учитывает особенности информационной системы, используемые в ней программные, программно-технические, технические средства и процессы обработки информации, дает описание угроз безопасности, которым подвержена информационная система.

В ходе ВКР были выделены наиболее существенные угрозы информационной безопасности и разработана модель угроз на основании документа «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка)» ФСТЭК [1].

Подробное описание модели угроз приведено в Приложении К.

1.7. Разработка технического задания на создание системы защиты персональных данных на предприятии ООО «Трехгорный керамический завод»

По результатам предпроектного обследования было разработано техническое задание на создание системы защиты персональных данных на предприятии ООО «Трехгорный керамический завод» (Приложение Б).

В качестве основы был взят ГОСТ 34.602-1989 «Техническое задание на создание автоматизированной системы» [3]. Техническое задание имеет следующие разделы:

– общие сведения;
– назначение и цели создания системы защиты персональных данных;
– характеристика объекта защиты;
– требования к СЗПДн;
– состав и содержание работ по созданию СЗПДн;
– порядок контроля и приемки системы;
– требования к документированию.

1.8. Уровень защищенности персональных данных

Акт определения уровня защищенности персональных данных является одним из документов, содержащих сведения о реализуемых требованиях к защите персональных данных.

Акт определения уровня защищенности персональных данных не является документом конфиденциального характера. Оператор персональных данных обязан

опубликовать или иным образом обеспечить неограниченный доступ к документу, содержащему сведения о реализуемых требованиях к защите персональных данных.

Для определения уровня защищенности персональных данных на предприятии должна быть создана комиссия. В состав комиссии обязательно должен быть включен ответственный за организацию обработки персональных данных. Комиссия должна быть назначена приказом руководителя. По результатам определения уровня защищенности персональных данных должен быть оформлен акт. Акт определения уровня защищенности персональных данных должен утверждаться руководителем предприятия (председатель и члены комиссии назначаются приказом о проведении внутренней проверки). Акт должен быть подписан всеми членами комиссии.

Акт определения уровня защищенности персональных данных составляется для каждой информационной системы персональных данных (ИСПДн) и прилагается к уведомлению об обработке (если уведомление необходимо). Для каждой ИСПДн должна быть определена ее структура, в которой определяются характеристики режима обработки.

На основании полученных данных каждой ИСПДн должен быть определен необходимый уровень защищенности персональных данных. Правильно выявить уровень защищенности необходимо для того, чтобы определить требования для обеспечения защиты ИСПДн. Определение уровня защищенности персональных данных проводится в соответствии с постановлением Правительства РФ от 01.11.2012 №1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

В акте указывается:

- обрабатываемые в ИСПДн персональные данные;
- объем обрабатываемых персональных данных;
- тип актуальных угроз для ИСПДн;
- уровень защищенности персональных данных.

Уровень защищенности определяется на основании обрабатываемых персональных данных в ИСПДн, объема, обрабатываемых данных и типа актуальных угроз.

В ИСПДн «Сотрудники» обрабатываются данные менее чем 100000 субъектов, являющихся сотрудниками оператора. Обрабатываемые категории персональных данных – иные ПДн. Тип актуальных угроз – 3.

На основании полученных данных для ИСПДн «Сотрудники» был определен 4 уровень защищенности, что отражено в акте определения уровня защищенности ПДн (Приложение М).

1.9. Вывод по первой главе

Первая глава посвящена анализу состояния защиты информации в ООО «Трехгорный керамический завод» и определению существующих угроз информационной безопасности. В качестве объекта защиты был выбран отдел кадров ООО «Трехгорный керамический завод», а также выявлена информация ограниченного доступа – персональные данные. Категория персональных данных – иные ПДн. Был проведен анализ информационной системы отдела с целью выявления объектов защиты.

Основываясь на перечне объектов защиты и «Базовой модели угроз безопасности информации при их обработке в ИСПДн» ФСТЭК России от 15 февраля 2008 г. была разработана модель угроз и уязвимостей и выявлены типы актуальных угроз:

- Доступ к информации, ее модификация и уничтожение лицами, не имеющими прав доступа.
- Воздействие вредоносных программ (вирусов).
- Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.
- Угроза выявления паролей по сети.
- Угрозы типа «Отказ в обслуживании».
- Угрозы внедрения по сети вредоносных программ.
- Угрозы удаленного запуска приложений.

ИСПДн данного предприятия недостаточно защищена, что, в результате, приводит к высокой опасности реализации этих угроз. Исходя из этого, необходимо принять меры по защите ПДн.

В соответствии с документом ФСТЭК России от 14 февраля 2008 г. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», был определен уровень защищенности ИСПДн – средний, а также вероятность реализации каждой из угроз.

В соответствии с постановлением правительства от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» был определен 4 уровень защищенности ИСПДн.

В результате анализа полученных данных было составлено техническое задание на разработку информационной системы персональных данных ООО «Трехгорный керамический завод».

2. ТЕОРЕТИЧЕСКОЕ ОБОСНОВАНИЕ ВЫБОРА СРЕДСТВ ЗАЩИТЫ

2.1. Обзор возможных методов устранения уязвимостей

Одним из этапов обеспечения защиты персональных данных, обрабатываемых в ИСПДн «Сотрудники», является определение и анализ используемых в настоящее время методов и средств, необходимых для устранения выявленных угроз и уязвимостей. Исходя из разработанной в пункте 1.6 данной работы модели угроз был составлен список актуальных угроз безопасности для ИСПДн «Сотрудники»:

– Доступ к информации, ее модификации и уничтожение лицами, не имеющими прав доступа
– воздействие вредоносных программ (вирусов);
– угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций испдн, топологии сети, открытых портов и служб, открытых соединений и др.;
– угроза выявления паролей по сети;
– угрозы типа «отказ в обслуживании»;
– угрозы внедрения по сети вредоносных программ;
– угрозы удаленного запуска приложений.

Рассмотрим наиболее эффективные варианты их устранения.

2.1.1. Угроза доступа к информации, ее модификации и уничтожение лицами, не имеющими прав доступа

Угроза осуществляется внешними нарушителями там, где расположены элементы ИСПДн и средства защиты, а также происходит работа пользователей.

Данную угрозу можно устранить установкой средства защиты от несанкционированного доступа (далее – НСД), прошедшего процедуру оценки соответствия требованиям ФСТЭК. Дополнительно в комплексе со средством защиты от НСД необходима реализация организационных и инженерно-технических мер, таких как:

– установка замков на дверь помещения, в котором ведется обработка персональных данных;
– установка тревожной кнопки.
– установка охранно-пожарной сигнализации;
– установка поста круглосуточной охраны;

Для определения оптимального средства защиты был проведен сравнительный анализ 2-х наиболее часто используемых средств защиты от НСД, приведенный в Таблице 4.

Таблица 4 – Сравнительный анализ средств защиты от НСД

Критерии сравнения Средств СЗИ	Dallas Lock 8.0-K	Secret Net 7
Стоимость, руб.	От 15000 (За 2 АРМ)	От 18000 (За 2 АРМ)
Наличие сертификата ФСТЭК	+	+
Срок действия сертификата ФСТЭК	ФСТЭК России № 2720 Действителен до 25.09.2018 г.	ФСТЭК России № 2707 Действителен до 07.09.2018 г.
Класс защищенности	По 5 классу защищенности	По 3 классу защищенности
Уровень контроля НДВ	По 4 уровню контроля	По 2 уровню контроля
Класс автоматизированных систем	До класса 1Г включительно	До класса 1Б включительно
Свободное место на жестком диске	1,030 Гб	2,000 Гб
Поддержка ОС семейства Windows	+	+

Исходя из данных таблицы, по техническим характеристикам СЗИ Secret Net 7 обладает явным преимуществом перед СЗИ Dallas Lock 8.0-K, но нужно учитывать, что характеристики Secret Net 7 являются избыточными для защиты данной ИСПДн, что в сумме с его более высокой стоимостью является менее приемлемым вариантом для рекомендации Secret Net 7 к покупке.

Учитывая все вышесказанное, в качестве средства от НСД для ИСПДн «Сотрудники» рекомендуется установка СЗИ от НСД Dallas Lock 8.0-K стоимостью 15000 рублей за 2 АРМ.

2.1.2. Угроза воздействия вредоносных программ (вирусов)

Программой с потенциально опасными последствиями или вредоносной программой (вирусом) называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять следующие функции [1]:

– скрывать признаки своего присутствия в программной среде компьютера;

– обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;

– разрушать (искажать произвольным образом) код программ в оперативной памяти;

– выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирования, уничтожения, блокирования и т.п.);

– сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);

– искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в

результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

Данную угрозу можно устранить установкой антивирусного средства, прошедшего процедуру оценки соответствия требованиям ФСТЭК.

Для принятия решения об установке оптимального средства антивирусной защиты был проведен сравнительный анализ 3-х наиболее часто используемых средств антивирусной защиты, приведенный в Таблице 5.

Таблица 5 – Сравнительный анализ средств антивирусной защиты

Критерии сравнения	Kaspersky Endpoint Security 10	Dr.Web Enterprise Security Suite версия 10.0	ESET NOD32 Secure Enterprise Pack 5.0
Стоимость, руб.	От 4000 (Для 2 АРМ)	От 8100 (Для 5 АРМ)	От 79400 (Для 30 АРМ)
Наличие сертификата	+	+	+
Срок действия сертификата ФСТЭК	№ 3025 действителен до 25.11.2019 года	№ 3509 действителен до 27.01.2019 года	№ 3243 действителен до 13.10.2020 года
Средний уровень обнаружения вредоносного	98.78%	91.50%	93.17%
Среднее время реакции на новые угрозы, часы	0-1.5	2-3	2-4
Лечение активного заражения	71%	82%	18%
Занимаемая оперативная память, мб	230	333	312
Среднее время сканирования, мин.	35	67	29

ESET NOD32 Secure Enterprise Pack 5.0 нецелесообразно рекомендовать к покупке ввиду его высокой стоимости и относительно слабых характеристик по сравнению с другими представленными продуктами. По данным таблицы 5 можно сделать вывод о том, что и Kaspersky Endpoint Security 10 и Dr.Web Enterprise Security Suite 10.0 обладают своими преимуществами. Но для данной ИСПДн наиболее выгодным и менее затратным решением будет установка Kaspersky Endpoint Security 10 для Windows, так как в данной ИСПДн присутствуют только 2 АРМ и лицензия от компании Kaspersky будет наиболее правильным выбором.

Исходя из всего вышесказанного, в качестве средства антивирусной защиты рекомендуется установка Kaspersky Endpoint Security 10 для Windows.

2.1.3. Угроза сканирования, направленная на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.

Сущность процесса реализации угрозы заключается в передаче запросов сетевым службам хостов ИСПДн и анализе ответов от них. Цель – выявление используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей.

Данную угрозу можно устранить установкой средства межсетевого экранирования, прошедшего процедуру оценки соответствия требованиям ФСБ.

Для того чтобы определиться со средством межсетевого экранирования, был проведен сравнительный анализ 2-х наиболее часто используемых средств межсетевого экранирования, приведенный в Таблице 6.

Таблица 6 – Сравнительный анализ средств межсетевого экранирования

Критерии сравнения	VipNet Client 4.0 (КС3)	Security Studio Endpoint Protection Personal Firewall	TrustAccess
Стоимость, руб.	От 7500	От 2900	От 2500
Наличие сертификата ФСБ	+	+	+
Срок действия сертификата	№ 3727 Действителен до 30.11.2019	№ 2901 Действителен до 25.07.2018	№ 2146 Действителен до 30.07.2019
Фильтрация доступа	да	да	да
Контроль доступа	да	нет	да
Контроль трафика	да	нет	нет
Контроль целостности	да	да	да
Защита до входа в систему	да	да	нет

Исходя из сравнительного анализа 3-х межсетевых экранов, несмотря на более высокую стоимость, рекомендуется установить программный комплекс VipNet Client 4.0 (КС3), так как данное средство имеет ряд преимуществ по сравнению с другими СЗИ, так как в состав программного комплекса ViPNet Client 4.0 входят:

– драйвер сетевой защиты, взаимодействующий непосредственно с драйвером сетевого интерфейса компьютера и осуществляющий контроль и фильтрацию трафика обмена компьютера с внешней сетью;

– сервис управления драйвером сетевой защиты, обеспечивающий функционирование узла в сети ViPNet;

– драйвер шифрования IP-пакетов, осуществляющий шифрование и имитозащиту IP-пакетов;

– приложение ViPNet Client Монитор, предоставляющее пользовательский интерфейс (GUI) для настройки параметров работы ПК ViPNet Client и программный интерфейс для взаимодействия с ПК ViPNet SafeDisk-V;

– сервис регистрации пользователя, обеспечивающий обработку событий аутентификации пользователя ПК ViPNet Client;

– транспортный модуль ViPNet MFTP, реализующий обмен управляющей, адресной и ключевой информацией с программным обеспечением централизованного управления сетью ViPNet (ПО ViPNet Administrator, ПО ViPNet Policy Manager), отправку, прием и маршрутизацию электронных документов (почтовых конвертов), отправку, прием и маршрутизацию электронных документов (почтовых конвертов);

– служба ViPNet Контроль приложений, осуществляющая контроль сетевой активности приложений и позволяющая реализовывать политики доступа приложений в сеть;

– прикладное ПО ViPNet Деловая почта для обмена зашифрованными и подписанными сообщениями.

2.1.4. Угроза выявления паролей по сети

Цель реализации угрозы состоит в получении НСД путем преодоления парольной защиты. Злоумышленник может реализовывать угрозу с помощью целого ряда методов, таких как простой перебор, перебор с использованием специальных словарей, установка вредоносной программы для перехвата пароля, подмена доверенного объекта сети (IP-spoofing) и перехват пакетов (sniffing). В основном для реализации угрозы используются специальные программы, которые пытаются получить доступ хосту путем последовательного подбора паролей. В случае успеха, злоумышленник может создать для себя «проход» для будущего доступа, который будет действовать, даже если на хосте изменить пароль доступа.

Данную угрозу можно минимизировать комплексным использованием антивирусного средства, а также средства межсетевого экранирования, прошедшего процедуру оценки соответствия требованиям ФСТЭК и ФСБ.

На основании проведенного анализа средств защиты в пунктах 2.1.2 и 2.1.3 настоящей работы, в качестве антивирусного средства рекомендуется установка Kaspersky Endpoint Security 10 для Windows, а в качестве средства межсетевого экранирования рекомендуется установить программный комплекс VipNet Client 4.0 (КС3).

2.1.5. Угроза типа «Отказ в обслуживании»

Эти угрозы основаны на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, когда операционная система оказывается не в состоянии обрабатывать поступающие пакеты.

Могут быть выделены несколько разновидностей таких угроз:

– скрытый отказ в обслуживании, вызванный привлечением части ресурсов ИСПДн на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований к времени обработки запросов. Примерами реализации угроз подобного рода могут служить: направленный шторм эхо-запросов по протоколу ICMP (Ping flooding), шторм запросов на установление TCP-соединений (SYN-flooding), шторм запросов к FTP-серверу;

– явный отказ в обслуживании, вызванный исчерпанием ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание), при котором легальные запросы не могут быть переданы через сеть из-за недоступности среды передачи, либо получают отказ в обслуживании ввиду переполнения очередей запросов, дискового пространства памяти и т.д. Примерами угроз данного типа могут служить шторм широковещательных ICMP-эхо-запросов (Smurf), направленный шторм (SYN-flooding), шторм сообщений почтовому серверу (Spam);

– явный отказ в обслуживании, вызванный нарушением логической связности между техническим средствами ИСПДн при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных (например, ICMP Redirect Host, DNS-flooding) или идентификационной и аутентификационной информации;

– явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа «Land», «TearDrop», «Bonk», «Nuke», «UDP-bomb») или имеющих длину, превышающую максимально допустимый размер (угроза типа «Ping Death»), что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

Результатом реализации данной угрозы может стать нарушение работоспособности соответствующей службы предоставления удаленного доступа к ПДн в ИСПДн, передача с одного адреса такого количества запросов на подключение к техническому средству в составе ИСПДн, которое максимально может «вместить»

трафик (направленный «шторм запросов»), что влечет за собой переполнение очереди запросов и отказ одной из сетевых служб или полная остановка ИСПДн из-за невозможности системы заниматься ничем другим, кроме обработки запросов.

Данную угрозу можно устранить установкой средства межсетевого экранирования, прошедшего процедуру оценки соответствия требованиям ФСБ.

На основании проведенного анализа средств защиты в пункте 2.1.3 настоящей работы, в качестве средства межсетевого экранирования рекомендуется установить программный комплекс VipNet Client 4.0 (КС3).

2.1.6. Угроза внедрения по сети вредоносных программ

К вредоносным программам, внедряемым по сети, относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. «Полноценные» сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, «подтолкнуть» пользователя к запуску зараженного файла.

Вредоносными программами, обеспечивающими осуществление НСД, могут быть:

- программы подбора и вскрытия паролей;
- программы, реализующие угрозы;
- программы, демонстрирующие использование недекларированных возможностей программного и программно-аппаратного обеспечения ИСПДн;
- программы-генераторы компьютерных вирусов;
- программы, демонстрирующие уязвимости средств защиты информации и др.

Данную угрозу можно устранить установкой антивирусного средства, прошедшего процедуру оценки соответствия требованиям ФСТЭК.

На основании проведенного анализа средств защиты в пункте 2.1.2 настоящей работы, в качестве антивирусного средства рекомендуется установка Kaspersky Endpoint Security 10 для Windows.

2.1.7. Угроза удаленного запуска приложений

Угроза заключается в стремлении запустить на хосте ИСПДн различные предварительно внедренные вредоносные программы: программы-закладки, вирусы, «сетевые шпионы», основная цель которых - нарушение конфиденциальности, целостности, доступности информации и полный контроль за работой хоста. Кроме

того, возможен несанкционированный запуск прикладных программ пользователей для несанкционированного получения необходимых нарушителю данных, для запуска управляемых прикладной программой процессов и др.

Выделяют три подкласса данных угроз:

– распространение файлов, содержащих несанкционированный исполняемый код;

– удаленный запуск приложения путем эксплуатации уязвимостей, например, путем переполнения буфера приложений-серверов;

– удаленный запуск приложения путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками, либо используемыми штатными средствами.

Типовые угрозы первого из указанных подклассов основываются на активизации распространяемых файлов при случайном обращении к ним. Примерами таких файлов могут служить: файлы, содержащие исполняемый код в вид документы, содержащие исполняемый код в виде элементов ActiveX, Java-апплетов, интерпретируемых скриптов (например, тексты на JavaScript); файлы, содержащие исполняемые коды программ. Для распространения файлов могут использоваться службы электронной почты, передачи файлов, сетевой файловой системы.

При угрозах второго подкласса используются недостатки программ, реализующих сетевые сервисы (в частности, отсутствие контроля за переполнением буфера). Настройкой системных регистров иногда удается переключить процессор после прерывания, вызванного переполнением буфера, на исполнение кода, содержащегося за границей буфера. Примером реализации такой угрозы может служить внедрение широко известного «вируса Морриса».

При угрозах третьего подкласса нарушитель использует возможности удаленного управления системой, предоставляемые скрытыми компонентами (например, «троянскими» программами типа Back. Orifice, Net Bus), либо штатными средствами управления и администрирования компьютерных сетей (Landesk Management Suite, Managewise, Back Orifice и т. п.). В результате их использования удается добиться удаленного контроля над станцией в сети.

Данную угрозу можно минимизировать комплексным использованием антивирусного средства, а также средства межсетевого экранирования, прошедшего процедуру оценки соответствия требованиям ФСТЭК и ФСБ.

На основании проведенного анализа средств защиты в пунктах 2.1.2 и 2.1.3 настоящей работы, в качестве антивирусного средства рекомендуется установка Kaspersky Endpoint Security 10 для Windows, а в качестве средства межсетевого экранирования рекомендуется установить программный комплекс VipNet Client 4.0 (КС3).

2.2. Вывод по второй главе

В результате выявленных уязвимостей в ИСПДн «Сотрудники», приводящих к реализации той или иной угрозы согласно составленной модели угроз и модели нарушителя безопасности персональных данных при их обработке в ИСПДн «Сотрудники» (Приложение К), были определены и рекомендованы мероприятия, препятствующие возникновению неблагоприятных последствий от выявленных угроз, а именно:

1. От угрозы доступа к информации, ее модификации и уничтожения лицами, не имеющими прав доступа: предложены организационные меры, а также установка программного комплекса средств защиты информации от несанкционированного доступа Dallas Lock 8.0-K;

2. От угрозы воздействия вредоносных программ (вирусов): предложена установка антивирусного средства Kaspersky Endpoint Security 10 для Windows;

3. От угроз сканирования, направленных на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.: предложена установка средства межсетевого экранирования программный комплекс VipNet Client 4.0 (КС3);

4. От угрозы выявления паролей по сети: предложена установка антивирусного средства Kaspersky Endpoint Security 10 для Windows, а также средства межсетевого экранирования программный комплекс VipNet Client 4.0 (КС3).

5. От угрозы типа «Отказ в обслуживании»: предложена установка средства межсетевого экранирования программный комплекс VipNet Client 4.0 (КС3);

6. От угрозы внедрения по сети вредоносных программ: предложена установка антивирусного средства Kaspersky Endpoint Security 10 для Windows;

7. От угрозы удаленного запуска приложений: предложена установка антивирусного средства Kaspersky Endpoint Security 10 для Windows, а также средства межсетевого экранирования программный комплекс VipNet Client 4.0 (КС3).

В результате оценки и выбора необходимых средств защиты информации для безопасного функционирования ИСПДн «Сотрудники» в ООО «Трехгорный керамический завод» было выявлено семь обязательных мероприятий, направленных на предотвращение и минимизацию угроз ПДн в ИСПДн «Сотрудники».

3. РАЗРАБОТКА ПРОЕКТА СИСТЕМЫ ЗАЩИТЫ ИСПДН НА ПРЕДПРИЯТИИ ООО «ТРЕХГОРНЫЙ КЕРАМИЧЕСКИЙ ЗАВОД»

3.1. Описание объекта

ООО «Трёхгорный керамический завод» производит алюмосиликатные пропанты средней прочности, изготовленные в соответствии с ГОСТ Р 51761-2013.

Производственная мощность завода на сегодняшний день составляет 30 000 тонн год. Использование в производстве современного оборудования в сочетании новейшими технологиями позволяет получать продукцию, не уступающую по своим показателям лучшим мировым образцам. Оптимизация технологических процессов начинается с подачи сырья в технологическую линию и заканчивается упаковкой готовой продукции. Соблюдение технологических показателей гарантировано системой контроля на основе аналитической лаборатории, которая отвечает всем требованиям ISO 9001.

На предприятии циркулирует информация о сотрудниках, контрагентах, заказах и технологиях. Основной информацией, обрабатываемой в отделе кадров предприятия, является ПДн сотрудников.

Структура защищаемой информации представлена в таблице 7.

Таблица 7 – Структура защищаемой информации.

Входящая	Исходящая
ПДн сотрудников	ПДн сотрудников
	Рабочие места
	Информация о занятости сотрудников
	Отчетность

3.2. Резюме проекта

Разработка проекта проводилась согласно утвержденному техническому заданию на создание системы защиты информационной системы ПДн в ООО «Трехгорный керамический завод» отдел кадров.

По мере реализации проекта необходимо разработать ряд программно-аппаратных и организационно-технических мер, а также матрицу ответственности, в которой указано, за какими лицами стоит ответственность за конкретные этапы разработки проекта. Определены основные объекты поставки.

Результатом проекта является защищенная автоматизированная система обработки персональных данных. Данная автоматизированная система соответствует

всем нормативно-правовым документам в области защиты ИБ и целям внедрения ИСПДн.

3.3. Цели и задачи проекта

Целями разработки ИСПДн на предприятии ООО «Трехгорный керамический завод» являются:

- предотвращение утечки и искажения информации;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;
- предотвращение других форм незаконного вмешательства в информационные ресурсы и системы, обеспечение правового режима информации как объекта собственности;
- защита персональных данных сотрудников предприятия в соответствии с требованиями действующих руководящих документов ФСТЭК России.

Задачами проекта являются:

- анализ процессов управления информационной безопасностью;
- развитие системы информационной безопасности в направлениях обеспечения организационно-технической и программно-аппаратной безопасности;
- реализация мероприятий по защите персональных данных сотрудников предприятия.

3.4. Объекты поставки проекта

Данный проект предусматривает создание документов по защите ПДн:

- должностные обязанности пользователей (сотрудников отдела кадров).
- политика обработки персональных данных.

К программно-аппаратным мерам относятся: средство защиты информации от НСД «Dallas Lock 8.0-k», антивирусное ПО «Kaspersky Endpoint security 10». Сотрудники отдела должны быть обучены новым требованиям по защите информации, которые представлены в организационно-распорядительных документах и вытекающих из новых аппаратно-технических решений. Обучение должно быть обосновано значимостью выполнения требований для организации.

3.5. Риски проекта

На первом этапе рассчитаем уровень угрозы Th (%), который зависит от следующих показателей:

- ER (%) – критичность реализации угрозы;

- $P(V)$ (%) – вероятность реализации угрозы через данную уязвимость. Уровень угрозы рассчитывается по формуле (2).

$Th = ER * P(V)$, (1)

В таблице 8 представлены уровни угроз проекта.

Таблица 8 – Уровень угрозы Th.

Риски	ER	$P(V)$	Th
Риски изменений в стране и обществе			
Реформы в экономике и политике	10	5	0.005
Изменение законодательства	15	5	0.007
Изменение здравоохранения и медицины	25	5	0.012
Изменение условий отдыха	25	5	0.012
Отрицательное отношение сотрудников	75	5	0.037
Риски в составе организации			
Задержки финансирования	90	10	0.09
Отсутствие резерва в случае реализации рисков	90	70	0.63
Отставание по срокам	10	10	0.01
Дефицит в рабочей силе	20	5	0.01
Увеличение стоимости работ	20	3	0.006
Риски, связанные с персоналом			
Личностные факторы	25	15	0.037
Риск, связанный с заменой сотрудников	10	5	0.005

На втором этапе для расчета уровня угроз по всем уязвимостям CTh, воспользуемся формулой (3):

$CTh = 1 - \prod i{=}1(1 - Th)$ (3)

Результаты расчетов уровня угроз по всем уязвимостям представлен в таблице 9.

Таблица 9 – Уровни угроз по всем уязвимостям.

Уровни угроз по уязвимостям	CTh
Риски изменений в стране и обществе	0.066
Риски в составе организации	0.671
Риски, связанные с персоналом	0.041

Из полученных значений уровня угроз по уязвимостям видно, что риски, связанные с изменениями в стране и обществе и риски, связанные с персоналом – малы. Риски в составе организации составляют 0.671, что имеет существенное значение.

3.6. Структура разбиения работ

Структура разбиения работ дает возможность согласовать план проекта с заказчиком. Структура представлена в виде описания работ.

Структура работ по совершенствованию ИСПДн:

- ИСПДн 1. Проектирование:
- ИСПДн 1.1. Определение ключевых показателей существующих бизнес-процессов с точки зрения ИБ;
- ИСПДн 1.2. Анализ проблем существующих бизнес-процессов;
- ИСПДн 1.3. Разработка значений ключевых показателей новых бизнес-процессов;
- ИСПДн 1.4. Выбор наилучших способов и методов улучшения значений ключевых показателей бизнес-процессов;
- ИСПДн 1.5. Разработка и согласование структуры новых бизнес-процессов;
  ИСПДн 2. Создание и модернизация организационно-распорядительной документации:
- ИСПДн 2.1. Положение «О ПДн»;
- ИСПДн 2.2. Внесение изменений в должностные инструкции;
- ИСПДн 2.3. Согласование и утверждение организационно-распорядительной документации;
- ИСПДн 3. Подготовка реализации проекта системы защиты ИСПДн:
- ИСПДн 3.1. Определение ответственных лиц и исполнителей проекта;
- ИСПДн 3.2. Приобретение программно-аппаратного средства защиты от НСД и антивирусного ПО;
- ИСПДн 4.Внедрение:
- ИСПДн 4.1. Установка и настройка программно-аппаратного средства защиты от НСД и антивирусного ПО;
- ИСПДн 4.2. Контроль защищенности;
- ИСПДн 4.3. Обучение пользователей.

Структурное разбиение работ представлено на рисунке 1.

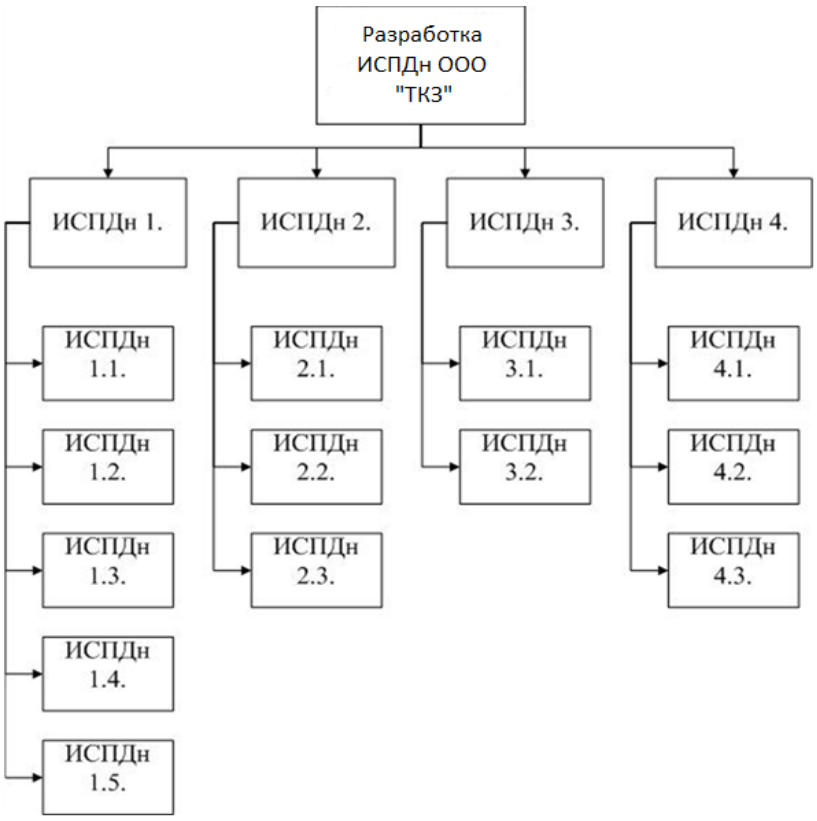

Рисунок 1 – Структурное разбиение работ.

3.7. Структурная схема организации проекта

Структурная схема организации проекта способствует точному и своевременному выполнению всех этапов работ проекта, скоординированного для взаимодействия всех сотрудников, вовлеченных в проект. Структурная схема организации проекта представлена на рисунке 2.

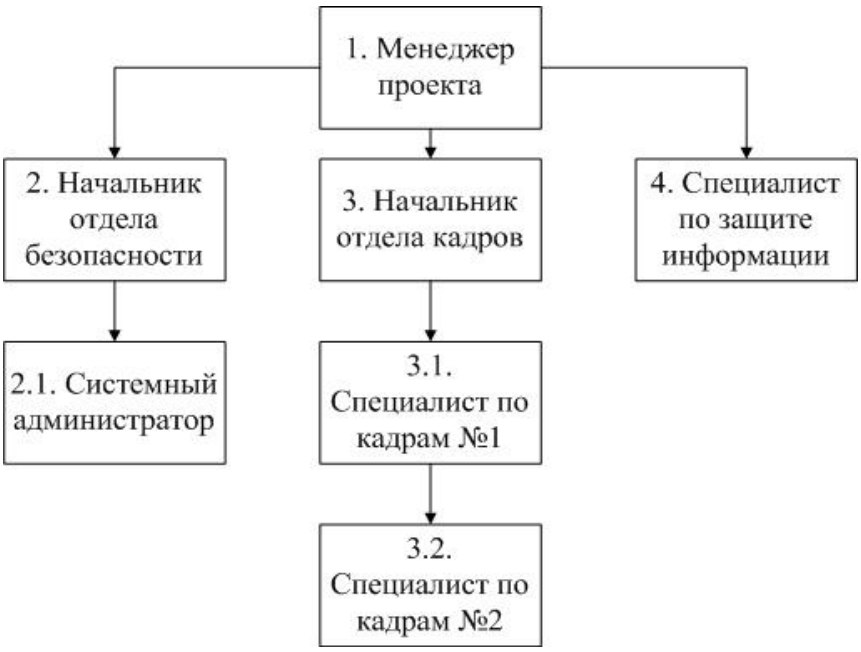

Рисунок 2 – Структурная схема организации проекта.

3.8. Матрица ответственности

На основании п. 3.6 и 3.7 построим матрицу ответственности. Действия исполнителей по работам делятся на следующие группы:

- управление (У);
- исполнение (И);
- контроль (К).

Матрица ответственности представлена в таблице 10.

Таблица 10 – Матрица ответственности.

Исполнитель Работа	1	2	2.1	3	3.1	3.2	4
1	2	3	4	5	6	7	8
ИСПДн 1.	К						
ИСПДн 1.1.	К, У	И					И
ИСПДн 1.2.	И						К
ИСПДн 1.3.	И						К
ИСПДн 1.4.	К, У	И					И
ИСПДн 1.5.	И						К
ИСПДн 2.	К	К					У, И
ИСПДн 2.1.	К	К					У, И
ИСПДн 2.2.	К	К					У, И
ИСПДн 2.3.	К	К					У, И

Продолжение таблицы 10

1	2	3	4	5	6	7	8
ИСПДн 3.	К						
ИСПДн 3.1.	К	И					И
ИСПДн 3.2.	К		И				
ИСПДн 4.	К		И				
ИСПДн 4.1.	К		И				
ИСПДн 4.2.	К	И					
ИСПДн 4.3.	И	К		К	К	К	К

3.9. Диаграмма Ганта и сетевой график

Для соответствия плану работ необходимо установить сроки выполнения работ. Для это составляется расписание выполнения работ. Расписание выполнения работ представлено в таблице 11.

Таблица 11 – Расписание выполнения работ.

Код работы	Работа	Длительность работы, дней	Ранний срок начала работы, дней	Поздний срок начала работы, дней	Ранний срок окончания работы, дней	Поздний срок окончания работы, дней
1	2	3	4	5	6	7
	Проектирование	17	0	0	17	17
1-2	Определение ключевых показателей существующих бизнес-процессов с точки зрения ИБ	4	0	0	4	4
2-3	Анализ проблем существующих бизнес-процессов	2	4	4	6	6
3-4	Разработка значений ключевых показателей новых бизнес-процессов	4	6	6	10	10
4-5	Выбор наилучших способов и методов улучшения значений ключевых показателей бизнес-процессов	3	10	10	13	13
5-6	Разработка и согласование структуры новых бизнес-процессов	4	13	13	17	17

Продолжение таблицы 11

	Создание организационно-распорядительной документации	8	17	17	25	25
6-7	Положение «О ПДн»	3	17	17	20	20
7-8	Внесение изменений в должностные инструкции	3	20	20	23	23
8-9	Согласование и утверждение организационно-распорядительной документации	2	23	23	25	25
	Подготовка реализации проекта системы защиты ИСПДн	1	25	25	26	26
9-10	Определение ответственных лиц и исполнителей проекта	1	25	25	26	26
10-11	Приобретение программно-аппаратного средства защиты от НСД	1	25	25	26	26
	Внедрение	2	26	26	28	28
11-12	Установка и настройка программно-аппаратного средства защиты от НСД и антивирусного ПО	1	26	26	27	27
12-13	Контроль защищенности	1	27	27	28	28
13-14	Обучение пользователей	1	27	27	28	28

Чтобы построить диаграмму Ганта, необходимо определить перечень задач и сроки их выполнения с учетом выходных дней, опираясь на сетевой график. Перечень задач и сроков представлен в таблице 12.

Таблица 12 – перечень задач и сроков.

Работа	Название работы	Длительность	Начало	Окончание
1	2	3	4	5
1	Проектирование	17	19.01.2018	13.02.2018

Продолжение таблицы 12

1	2	3	4	5
1.1	Определение ключевых показателей существующих бизнес-процессов с точки зрения ИБ	4	19.01.2018	25.01.2018
1.2	Анализ проблем существующих бизнес-процессов	2	25.01.2018	27.01.2018
1.3	Разработка значений ключевых показателей новых бизнес-процессов	4	27.01.2018	2.02.2018
1.4	Выбор наилучших способов и методов улучшения значений ключевых показателей бизнес-процессов	3	2.02.2018	7.02.2018
1.5	Разработка и согласование структуры новых бизнес-процессов	4	7.02.2018	13.02.2018
2	Создание и модернизация организационно-распорядительной документации	8	13.02.2018	23.02.2018
2.1	Положение «О ПДн»	3	13.02.2018	16.02.2018
2.2	Внесение изменений в должностные инструкции	3	16.02.2018	21.02.2018
2.3	Согласование и утверждение организационно-распорядительной документации	2	21.02.2018	23.02.2018
3	Подготовка реализации проекта системы защиты ИСПДн	1	23.02.2018	24.02.2018
3.1	Определение ответственных лиц и исполнителей проекта	1	23.02.2018	24.02.2018
3.2	Приобретение программно-аппаратного средства защиты от НСД	1	23.02.2018	24.02.2018
4	Внедрение	2	24.02.2018	28.02.2018
4.1	Установка и настройка программно-аппаратного средства защиты от НСД и антивирусного ПО	1	24.02.2018	27.02.2018
4.2	Контроль защищенности	1	27.02.2018	28.02.2018
4.3	Обучение пользователей	1	27.02.2018	28.02.2018

На основании таблицы 15 построим диаграмму Ганта. Диаграмма Ганта представлена на рисунке 3.

Из расписания выполнения работ видно, что срок проекта составляет 28 дней. На диаграмме Ганта указаны сроки выполнения всех работ с учетом выходных и праздничных дней. Сроки реализации проекта – 19.01.2018 – 28.02.2018.

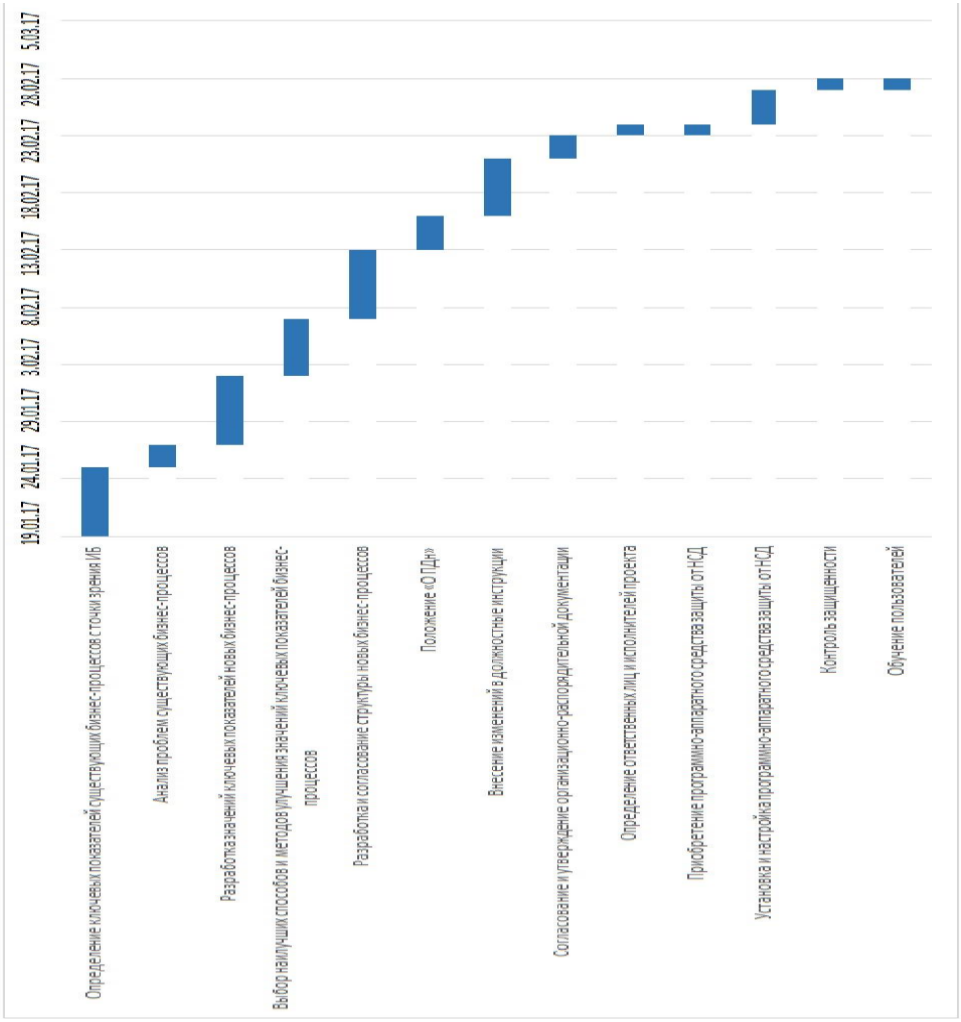

Рисунок 3 – Диаграмма Ганта.

3.10. Расчет бюджета проекта

В результате предпроектного обследования были выявлены уязвимости в системе, в связи с чем необходимо их устранить, организовав систему защиты. Был проведен расчёт затрат на реализацию предложенных мер защиты. В таблице 13 представлена стоимость оборудования и программного обеспечения.

Таблица 13 – Стоимость оборудования и программного обеспечения

Наименование	Цена за шт. (руб.)	Количество	Сумма (руб.)
СЗИ от НСД «Dallas lock 8.0-k»	7500	1	7500
СЗИ от НСД «Dallas lock 8.0-k» с модулем межсетевой экран	9000	1	9000
Kaspersky Endpoint Security 10	2000	2	4000
VipNet Client 4.0 (КС3)	7500	1	7500
Итог	-	-	28000

Стоимость реализации проекта приведена в таблице 14

Таблица 14 – Стоимость реализации проекта

Наименование	Стоимость (руб.)
Анализ существующей СЗИ	0
Разработка организационно-распорядительной документации	0
Установка и настройка антивирусного ПО «Kaspersky End-point Security 10 для Windows»	0
Установка и настройка СЗИ от НСД «Dallas Lock 8.0-K»	0
Установка и настройка межсетевого экрана «VipNet Client 4.0»	4000
Итог	4000

Затраты на реализацию проекта по организации системы защиты ИСПДн «Сотрудники» в ООО «Трехгорный керамический завод» составили 32000 рублей.

3.11. Вывод по третьей главе

Результатом третьей главы является разработанный проект по созданию системы защиты ИСПДн на предприятии ООО «Трехгорный керамический завод». Составлено описание объекта, что позволяет определить структуру защищаемой информации.

Определены цели проекта:

- Защита автоматизированной системы обработки персональных данных в ООО «Трехгорный керамический завод».
- Исследование рисков проекта, в ходе которого выяснилось, что наиболее существенными рисками являются риски в составе организации.

Работы по реализации проекта были последовательно распределены. Каждой из них был назначен ответственный за выполнение. Графики выполнения работ наглядно представлены на диаграмме Ганта.

В результате расчета всех затрат на организацию защиты ИСПДн «Сотрудники» ООО «Трехгорный керамический завод» необходимо 32000 рублей. Реализация проекта позволит выполнить требования законодательства в области защиты персональных данных. Из этого можно сделать вывод, что проект по организации защиты персональных данных в ИСПДн ООО «Трехгорный керамический завод» необходим и целесообразен.

Проект включает введение разработанных организационно-технических и программно-аппаратных мер по защите ПДн в ИСПДн.

ЗАКЛЮЧЕНИЕ

В результате проделанной работы была создана защищенная система персональных данных в ООО «Трехгорный керамический завод». В ходе разработки было проведено обследование организации, в рамках которого была установлена специфика деятельности, особенности и характеристики, а также возможные уязвимости и угрозы, стоящие перед организацией.

По результатам обследования был разработан пакет документов, включающий в себя:

- акт определения уровня защищенности ИСПДн «Сотрудники» (Приложение М);
- организационно-распорядительную и эксплуатационную документацию (Приложения Г-И);
- модель угроз для ИСПДн «Сотрудники» (Приложение К);
- техническое задание для ИСПДн «Сотрудники» (Приложение Б).

Проведение мероприятий по созданию системы защиты персональных данных показало, что внедрение новых организационных мер и технических средств оказывает влияние на привычный процесс работы, что говорит о необходимости проведения дополнительного обучения персонала организации.

В качестве объекта защиты был выбран отдел кадров ООО «Трехгорный керамический завод», а также выявлена информация ограниченного доступа – персональные данные. Категория персональных данных – иные ПДн. Был проведен анализ информационной системы отдела с целью выявления объектов защиты.

Основываясь на перечне объектов защиты и «Базовой модели угроз безопасности информации при их обработке в ИСПДн» ФСТЭК России от 15 февраля 2008 г. была разработана модель угроз и уязвимостей и выявлены типы актуальных угроз:

- Доступ к информации, ее модификация и уничтожение лицами, не имеющими прав доступа.
- Воздействие вредоносных программ (вирусов).
- Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.
- Угроза выявления паролей по сети.
- Угрозы типа «Отказ в обслуживании».
- Угрозы внедрения по сети вредоносных программ.
- Угрозы удаленного запуска приложений.

В соответствии с документом ФСТЭК России от 14 февраля 2008 г. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», был определен уровень защищенности ИСПДн – средний, а также вероятность реализации каждой из угроз.

В соответствии с постановлением правительства от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» был определен 4 уровень защищенности ИСПДн.

При проектировании системы защиты был произведен выбор технических средств защиты информации. В качестве средства защиты от несанкционированного доступа, было выбрано сертифицированное средство Dallas Lock 8.0-K, т.к. оно является простым в эксплуатации, надежным и поддерживается всеми рабочими станциями оператора. В качестве средства межсетевого экранирования было выбрано сертифицированное средство VipNet Client 4.x, т.к. оно обеспечивает высокий уровень надежности и идеально совместимо с СЗИ от НСД Dallas Lock 8.0-K. Средства СЗИ были установлены и настроены в соответствии с инструкциями предоставленными разработчиками, моделью угроз и техническим заданием на ИСПДн. Для предотвращения оставшихся угроз были приняты организационно-правовые меры.

Также с целью ускорения адаптации сотрудников к новым особенностям информационного взаимодействия, было предусмотрено обучение. До сотрудников был донесен порядок работы с персональными данными, средствами защиты информации, в том числе антивирусными. Сотрудники были ознакомлены со всеми составленными инструкциями, требованиями, изложенными в них, а также мерами ответственности за нарушение данных требований. Были подписаны обязательства о неразглашении защищаемой информации, а также листы ознакомления, свидетельствующие о знании сотрудником своих обязанностей и ответственности.

В рамках организационных мер были назначены сотрудники на должности администратора безопасности ИСПДн и ответственного за организацию обработки ПДн. Данные меры были приняты, чтобы реализовать принцип персональной ответственности, необходимый для создания эффективной системы защиты.

Все мероприятия по защите персональных данных были документально отражены. Уязвимость отсутствия программных и (или) аппаратных средств защиты конфиденциальной информации была закрыта путем установки на рабочие места сотрудников в обоих ИСПДн сертифицированных СЗИ. Уязвимость, выраженная в отсутствии антивирусных проверок после установки и (или) изменения какого-либо ПО была минимизирована созданием и утверждением инструкции пользователя ИСПДн, в которой был регламентирован порядок предотвращения вирусного

заражения ИСПДн. Отсутствие регламента доступа в защищенные помещения было компенсировано созданием и утверждением инструкции о порядке работы с ПДн. Аналогичным образом были закрыты все выявленные уязвимости и сведены к допустимому минимуму обнаруженные угрозы безопасности персональным данным.

Работы по реализации проекта были последовательно распределены и каждой из них был назначен ответственный за выполнение. Графики выполнения работ были наглядно представлены на диаграмме Ганта. Из расписания выполнения работ видно, что срок проекта составляет 28 рабочих дней.

В результате расчета всех затрат на организацию защиты ИСПДн «Сотрудники» ООО «Трехгорный керамический завод» необходимо 32000 рублей. Реализация проекта позволит выполнить требования законодательства в области защиты персональных данных. Из этого можно сделать вывод, что проект по организации защиты персональных данных в ИСПДн ООО «Трехгорный керамический завод» необходим и целесообразен.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Нормативно-правовые документы

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Выписка). Утверждена ФСТЭК России 15.02.2008.

2. ГОСТ 2.051-2006 Единая система конструкторской документации. Электронные документы. Общие положения. Введен 01.09.2006 – М: Изд-во стандартов, 2007 – 12 с.

3. ГОСТ 34.602-89 Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы. Введен 24.03.1989 – М: Изд-во стандартов, 2006 – 10 с.

4. Гражданский кодекс Российской Федерации.

5. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК Российской Федерации 14.02.2008.

6. О Декларации прав и свобод человека и гражданина: утв. Постановлением Верховного совета РСФСР от 22 ноября 1991 года № 1920-1// Ведомости СНД РСФСР и ВС РСФСР.-1991.- № 52.- Ст. 1865.

7. О персональных данных: Федер. закон Рос. Федерации от 27 июля 2006 г. № 152-ФЗ // Рос. газ. – 2006. – 29 июля.

8. Об информации, информационных технологиях и о защите информации: Федер. закон Рос. Федерации от 27 июля 2006 г. № 149-ФЗ // Рос. газ. – 2006. – 29 июля.

9. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»: приказ ФСТЭК России от 18 февраля 2013 г. N 21.

10. Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти: утв. Постановлением Правительства от 3 ноября 1994 г. № 1233.

11. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации: Гостехкомиссия РФ от 30 марта 1992 г.

12. Методика определения угроз безопасности информации в информационных системах (ПРОЕКТ). Утверждена ФСТЭК России 15.02.2015.

13. Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ.

14. СТО ЮУрГУ 04-2008 Стандарт организации. Курсовое и дипломное проектирование. Общие требования к содержанию и оформлению. Принят 10.12.2007 – Челябинск: Изд-во ЮУрГУ, 2008 – 56 с.

15. Требования к защите персональных данных при их обработке в информационных системах персональных данных: утв. Постановлением Правительства от 1 ноября 2012 г. №1119.

Основная литература

16. Dallas Lock система защиты информации от несанкционированного доступа [Электронный ресурс]. – http://www.dallaslock.ru/. – Загл. с экрана.

17. Secret Net система защиты информации от несанкционированного доступа [Электронный ресурс]. – Режим доступа: http://www.securitycode.ru/products/secret_net/. – Загл. с экрана.

18. Security Studio Endpoint Protection – сертифицированный антивирус, анти спам и анти шпион [Электронный ресурс]. – Режим доступа: http://www.securitycode.ru/products/security_studio_endpoint_protection/. – Загл. с экрана.

19. Вельдер, И.А. Система правовой защиты персональных данных в Европейском союзе: Автореф. дис. канд. юрид. наук. Казань. 2006. с.27.

20. Глушкова, С.И. Права человека в России: теория, история, практика: учеб. Пособие. Екатеринбург. 2002. с.748.

21. Лушников, А.М. Защита персональных данных работника: сравнительно-правовой комментарий гл.14 Трудового кодекса РФ // Трудовое право. 2009. № 9. С. 93-101.

22. Савинцева М. Правовая защита персональной информации граждан в России // Законодательство и практика масс-медиа. - 2006. - № 9. [Электронный ресурс]. – Режим доступа: http://www.law.edu.ru/doc/document.asp?docID=1239231 – Загл. с экрана.

23. Савчук, В.П. Оценка эффективности инвестиционных проектов: учебное пособие/ В.П. Савчук – М.: Финансы и статистика,1999.-158с.

ПРИЛОЖЕНИЕ А

УТВЕРЖДАЮ
Генеральный директор Общества с ограниченной ответственностью «Трехгорный керамический завод»
_____
«____» _____ 2018 г.

ТЕХНИЧЕСКИЙ ПАСПОРТ
на объект информатизации
АС «СОТРУДНИКИ»

Общества с ограниченной ответственностью «Трехгорный керамический завод»

СОСТАВИЛ

_____Е.В. Горбатова

«____» _____ 2018 г.

2018 г

I. ОБЩИЕ СВЕДЕНИЯ ОБ ИНФОРМАЦИОННОЙ СИСТЕМЕ

1.1. Наименование информационной системы персональных данных

Информационная система персональных данных «Сотрудники» (далее – ИСПДн «Сотрудники») принадлежит ООО «Трехгорный керамический завод».

1.2. Местонахождение ИСПДн

Информационная система располагается по адресу: 456082, г. Трехгорный Челябинской области, ул. Заречная, 1А, а/я 254.

1.3. Уровень защищенности персональных данных ИСПДн

Для персональных данных ИСПДн «Сотрудники» определен уровень защищенности – 4.

1.4. Сведения о контролируемой зоне

Для информационной системы определена граница контролируемой зоны, которой являются: ограждающие конструкции здания заводоуправления ООО «Трехгорный керамический завод».

II. СОСТАВ ИНФОРМАЦИОННОЙ СИСТЕМЫ

2.1. ИСПДн «Сотрудники», принадлежащая ООО «Трехгорный керамический завод», включает:

— основные технические средства и системы (ОТСС) в составе, приведенном в главе IV (перечень автоматизированных рабочих мест);

— системные и прикладные программные средства, установленные на автоматизированных рабочих местах, в составе, приведенном в главе VI;

— средства защиты информации, в составе, приведенном в главе VII.

III. ПЕРЕЧЕНЬ АВТОМАТИЗИРОВАННЫХ РАБОЧИХ МЕСТ

3.1. Перечень основных технических средств и систем (ОТСС) объекта информатизации отражен в таблице 1.

Таблица №1 – Перечень ОТСС, входящих в состав АС «СОТРУДНИКИ»

№ п/п	Название АРМ	Вид оборудования	Модель	Инвентарный (заводской) номер	Расположение
4.	АРМ Афанасьева	Системный блок	Microlab	FGH3457788HJIH	Кабинет отдела кадров
		Монитор	Aser	GHFTG4568JFF	
		Клавиатура	Logitech	TDE45678999JHG	
		Мышь	Smartbuy	REWD341178JKLK	
		Принтер	HP LaserJet P2055	FHFTHG428FGJ	
5.	АРМ Лапина	Системный блок	Microlab	FLWYO5867BHF	Кабинет отдела кадров
		Монитор	Aser	FOPPQW30905G	
		Клавиатура	Logitech	AWRG567KNG	
		Мышь	Aquarius	FH56333GHYOI	
		МФУ	Canon	DGRDHG56754G	

3.2. Перечень вспомогательных технических средств и систем (ВТСС) объекта, установленных в помещении объекта информатизации отражен в таблице 2.

Таблица №2 – Перечень ВТСС, входящих в состав АС «СОТРУДНИКИ»

№ п/п	Вид оборудования	Модель	Инвентарный номер	Расположение
1	Телефонный аппарат	Panasonic	GJDH233J	Кабинет отдела кадров
2	Телефонный аппарат	Panasonic	ETF3473FG	
3	Коммутатор	D-Link	EKRS453G	
4	Датчик пожарной сигнализации	-	-	
5	Датчик пожарной сигнализации	-	-	

IV. ПЕРЕЧЕНЬ ОБЩЕСИСТЕМНОГО И ПРИКЛАДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ИСПОЛЬЗУЕМОГО В ИНФОРМАЦИОННОЙ СИСТЕМЕ

4.1. Состав используемого общесистемного и прикладного программного обеспечения, используемого в информационной системе для обработки защищаемой информации представлен в таблице №3.

Таблица №3 – Перечень общесистемного и прикладного программного обеспечения

№ п/п	Наименование	Место установки	Примечание
1.	1С. Кадры	АРМ Афанасьева, АРМ Лапина	
2.	Microsoft Windows 7		
3.	Microsoft office 2007		
4.	Spu_orb		
5.	AVG Antivirus free		

V. СХЕМА РАСПОЛОЖЕНИЯ ОСНОВНЫХ ТЕХНИЧЕСКИХ СРЕДСТВ И СИСТЕМ

5.1. Места расположения технических средств, участвующих в обработке защищаемой информации, указаны на рисунке 1:

Рисунок №1 – Расположение ОТСС, ВТСС и границы контролируемой зоны ИС, располагающейся в кабинете отдела кадров

Границами контролируемой зоны являются ограждающие конструкции корпуса заводоуправления Общества с ограниченной ответственностью «Трехгорный керамический завод», находящийся по адресу: Челябинская обл., г. Трехгорный, ул. Заречная, д. 1А, согласно приказу «Об определении границ контролируемой зоны объекта информатизации АС «СОТРУДНИКИ» № 77 от 11.02.2018 г.

Кабинет располагается на втором этаже, окна завешаны жалюзи. Минимальное расстояние от ОТСС до КЗ составляет 2 метра.

VI. СВЕДЕНИЯ О СООТВЕТСТВИИ ТРЕБОВАНИЯМ ПО БЕЗОПАСНОСТИ ИНФОРМАЦИИ

6.1. Сведения об аттестации ИС на соответствие требованиям по безопасности информации представлены в таблице №5.

Таблица №5 – Сведения об аттестации информационной системы

№ п/п	Название документа	Уч. № документа	Дата
1.	Методики аттестационных испытаний информационной системы персональных данных		
2.	Программа аттестационных испытаний на соответствие требованиям по безопасности информации		
3.	Протокол аттестационных испытаний на соответствие требованиям по защите от НСД		
4.	Заключение по результатам аттестационных испытаний ОВТ		
5.	Аттестат соответствия требованиям по безопасности информации ИСПДн		

VII. РЕЗУЛЬТАТЫ ПЕРЕОДИЧЕСКОГО КОНТРОЛЯ

7.1. Результаты проведения периодического контроля информационной системы представлены в таблице №6.

Таблица №6 – Учет проведения регламентных работ

№ п/п	Наименование организации, проводившей проверку	Дата проведения проверки	Номер протокола	Примечание

VIII. РЕГИСТРАЦИЯ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ

8.1. Все произведенные изменения и дополнения в информационной системе представлены в таблице 7.

Таблица №7 – Регистрация изменений и дополнений

№ п/п	Дата введения изменений	Наименование документа, на основании которого вводятся изменения	Номера замененных (исправленных) листов технического паспорта	Подпись лица, внесшего изменения

ПРИЛОЖЕНИЕ Б

«УТВЕРЖДАЮ»
Генеральный директор
ООО «Трехгорный
керамический завод»
В.Ю. Горбатов
«___» _____2017 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
на создание системы защиты персональных данных на предприятии ООО «Трехгорный керамический завод»

1 ОБЩИЕ СВЕДЕНИЯ

1.1. Настоящее техническое задание разработано для информационной системы персональных данных «Сотрудники» ООО «Трехгорный керамический завод» и описывает требования, предъявляемые к построению, внедрению системы защиты персональных данных.

1.2. Полное наименование и обозначение системы: Система защиты информации, обрабатываемой в информационной системе персональных данных «Сотрудники».

1.3. Сокращенное наименование системы: СЗПДн

1.4. Предприятие разработчик системы: ООО «Трехгорный керамический завод», в лице главного специалиста по защите информации.

1.5. Предприятие заказчик системы: ООО «Трехгорный керамический завод», в лице генерального директора.

1.6. Работы по созданию СЗПДн проводятся на основании настоящего технического задания

1.7. При разработке технического задания (далее - ТЗ) использовались следующие нормативно-технические документы и методические материалы:

а) Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

б) Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

в) Постановление Правительства РФ от 01 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

г) Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

д) Приказ Гостехкомиссии России от 30 августа 2002 г. № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)»;

е) Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

ж) Приказ ФСБ России от 10 июля 2014 г. №378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

з) Руководящий документ ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

2 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1 Назначение системы защиты персональных данных (далее - СЗПДн):

2.1.1. Назначением СЗПДн является обеспечение информационной безопасности (далее - ИБ) персональных данных (далее - ПДн), обрабатываемых в информационной системе персональных данных (далее - ИСПДн).

2.1.2. СЗПДн призвана обеспечить конфиденциальность, целостность, доступность ПДн при их обработке в ИСПДн.

2.1.3. Объектом защиты СЗПДн является ИСПДн, описание которой приведено в частной модели угроз и модели нарушителя безопасности персональных данных информационной системы персональных данных (далее – Модель угроз).

2.2 Цели создания СЗПДн:Целями создания СЗПДн являются:

а) обеспечение защищенности ИСПДн в процессе обработки и хранения ПДн, а также обеспечение конфиденциальности ПДн при их обработке, а также других необходимых характеристик защищенности информации;

б) соответствие требованиям обеспечения ИБ при обработке ПДн в ИСПДн, регламентируемых РД ФСТЭК России и ФСБ России.

2.2.2 В результате создания СЗПДн должно быть обеспечено:

а) нейтрализация актуальных угроз информационной безопасности ПДн;

б) определение подлинности субъекта доступа, отслеживание действий субъектов доступа.

2.2.3 Критериями оценки достижения поставленных целей по созданию СЗПДн являются:

а) соответствие требованиям по обеспечению безопасности ПДн в ИСПДн, согласно приказу ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», для которых определен уровень защищенности, согласно Постановлению Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

б) соответствие требованиям приказа ФСБ России от 10 июля 2014 г. №378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

в) выполнение функциональных требований настоящего ТЗ;

г) проведение аттестационных испытаний ИСПДн на соответствие требованиям по безопасности информации и выдача аттестата соответствия.

3 ХАРАКТЕРИСТИКА ОБЪЕКТА ЗАЩИТЫ

3.1. Объектом защиты являются ПДн, обрабатываемые в ИСПДн «Сотрудники».

3.2. Категория обрабатываемых персональных данных – <иные ПДн>;

3.3. Тип актуальных угроз – 3;

3.4. Актуальные угрозы ИБ, которым подвержена ИСПДн «Сотрудники», определяются и обосновываются в Модели угроз, разрабатываемой Исполнителем на этапе проектирования ИСПДн на основе Руководящего документа ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

3.5. Для ПДн при их обработке в ИСПДн «Сотрудники» определен 4 уровень защищенности в соответствии с Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

3.6. Рабочие станции пользователей функционируют под управлением операционных систем Windows 7 Professional. Общее количество АРМ – 2.

4 ТРЕБОВАНИЯ К СЗПДН

4.1 Требования к СЗПДн в целом

4.1.1 Требования к структуре и функционированию

4.1.1.1 В состав СЗПДн должны входить следующие подсистемы:

а) идентификации и аутентификации субъектов доступа и объектов доступа;

б) управления доступом субъектов доступа к объектам доступа;

в) защиты машинных носителей информации,

г) регистрации событий безопасности;

д) антивирусной защиты;

е) анализа защищенности;

ж) защиты технических средств;

з) защиты информационной системы, ее средств, систем связи и передачи данных;

4.1.1.2 Структура СЗПДн может изменяться и уточняться по результатам разработки Модели угроз на предпроектной стадии с учетом обоснования необходимых изменений в ТЗ.

4.1.1.3 *Подсистема идентификации и аутентификации субъектов доступа и объектов доступа.* Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

4.1.1.4 *Подсистема управления доступом*. Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

4.1.1.5 *Подсистема защиты машинных носителей информации*. Меры по защите машинных носителей информации (средства обработки (хранения) информации, съемные машинные носители информации) должны исключать возможность несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированное использование съемных машинных носителей информации.

4.1.1.6 *Подсистема регистрации и учета*. Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

4.1.1.7 *Подсистема антивирусной защиты*. Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной

компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

4.1.1.8 *Подсистема контроля (анализа) защищенности информации*. Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по анализу защищенности информационной системы и тестированию ее системы защиты информации.

4.1.1.9 *Подсистема защиты технических средств*. Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационной системы (далее – средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей.

4.1.1.10 *Подсистема зашиты информационной системы, ее средств, систем связи и передачи данных*. Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту информации при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы, проектных решений по ее системе защиты информации, направленных на обеспечение защиты информации.

4.1.2 Требования к численности и квалификации персонала ИСПДн, режиму его функционирования

4.1.2.1 Квалификация персонала должна быть достаточной для осуществления им настройки общесистемных и сетевых сервисов СЗПДн и настройки СЗИ СЗПДн.

4.1.2.2 Персонал СЗПДн должен осуществлять обслуживание и эксплуатацию СЗПДн по рабочим дням в рабочее время, с возможностью выхода в нерабочее время для проведения сервисного обслуживания или восстановления работоспособности СЗПДн.

4.1.3 Показатели назначения

4.1.3.1 Системно-технические решения СЗПДн должны обеспечить минимизацию вероятности реализации угроз, описанных в Модели угроз для данной ИСПДн.

4.1.3.2 Экономический эффект от создания СЗПДн должен проявляться в снижении вероятной величины материального и морального ущерба по отношению к субъектам и оператору ПДн.

4.1.4 Требования к надежности

4.1.4.1 Должна быть обеспечена возможность резервного копирования конфигураций и журналов регистрации событий компонентов СЗПДн.

4.1.4.2 Аппаратно-программные компоненты СЗПДн должны функционировать в круглосуточном режиме и позволять осуществлять выполнение процедур резервирования и восстановления системы после сбоев.

4.1.5 Требования безопасности

4.1.5.1 Конструкция используемого оборудования должна обеспечивать защиту эксплуатирующего персонала от поражения электрическим током.

4.1.5.2 Размещение оборудования на штатных местах должно обеспечивать его безопасное обслуживание и эксплуатацию.

4.1.6 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов СЗПДн

4.1.7.1 Эксплуатация программно-технических средств должна предусматривать следующие виды технического обслуживания:

а) оперативное обслуживание;

б) профилактические работы.

4.1.7.2 Оперативное обслуживание должно предусматривать ежедневный контроль функционирования аппаратно-технических средств. Оперативное обслуживание не должно нарушать выполнения функций СЗПДн в целом.

4.1.7.3 Профилактическое обслуживание должно предусматривать периодическую проверку и обслуживание составных частей СЗПДн, для которых такое обслуживание предусмотрено эксплуатационной документацией.

4.1.7.4 Объем и порядок выполнения технического обслуживания технических и программных средств СЗПДн должны определяться эксплуатационной документацией.

4.1.7.5 Физический доступ неуполномоченных лиц к сетевому и серверному оборудованию должен быть запрещен.

4.1.7.6 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению могут уточняться на этапе проектирования СЗПДн.

4.1.7 Требования по сохранности информации при авариях

Сохранность информации при авариях в СЗПДн должна обеспечиваться методом резервного копирования.

4.1.8 Требования к стандартизации и унификации

4.1.11.1 Решения по использованию технических средств и ПО в СЗПДн должны использовать однотипные компоненты в целях обеспечения снижения расходов на обслуживание и ремонт, взаимозаменяемости используемых компонентов, удобства эксплуатации.

4.1.11.2 Должна обеспечиваться совместимость технических средств и ПО СЗПДн с техническими средствами и ПО, используемыми в ИСПДн «Сотрудники».

4.1.11.3 При применении технических средств и ПО особое внимание должно быть уделено унификации программных и аппаратных решений. Предпочтение должно отдаваться использованию готовых, проверенных на практике решений.

4.1 Требования к функциям, выполняемым СЗПДн

4.2.1 Подсистема идентификации и аутентификации субъектов доступа и объектов доступа (ИАФ)

В подсистеме должны обеспечиваться:

1) идентификация и аутентификация пользователей, являющихся работниками оператора (ИАФ.1);

2) управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов (ИАФ.3);

3) управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации (ИАФ.4);

4) защита обратной связи при вводе аутентификационной информации (ИАФ.5);

Для реализации подсистемы должны использоваться:

– организационные меры защиты информации;

– средства защиты информации от несанкционированного доступа, имеющие действующий сертификат соответствия требованиям, предъявляемым к средствам вычислительной техники не ниже 5 класса.

4.2.2 Подсистема управления доступом субъектов доступа к объектам доступа (УПД)

В подсистеме должны обеспечиваться:

5) управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей (УПД.1);

6) реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа (УПД.2);

7) управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами (УПД.3);

8) разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы (УПД.4);

9) назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы (УПД.5);

10) ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) (УПД.6);

11) Регламентация и контроль использования в информационной системе технологий беспроводного доступа (УПД.14);

Для реализации подсистемы должны использоваться:

– организационные меры защиты информации;

– средства защиты информации от несанкционированного доступа, имеющие действующий сертификат соответствия требованиям ФСТЭК, предъявляемым к средствам вычислительной техники не ниже 5 класса;

– средства межсетевого экранирования, имеющие действующий сертификат соответствия требованиям ФСТЭК (ФСБ), предъявляемым к межсетевым экранам не ниже 5 класса;

– средства защиты каналов передачи данных, имеющие действующий сертификат соответствия требованиям ФСБ, предъявляемым к средствам криптографической защиты информации.

4.2.3 Подсистема защиты машинных носителей информации (ЗНИ)

В подсистеме должны обеспечиваться:

12) учет машинных носителей информации (ЗНИ.1);

13) управление доступом к машинным носителям информации (ЗНИ.2);

14) уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) (ЗНИ.8).

Для реализации подсистемы должны использоваться:

– организационные меры защиты информации;

– средства защиты информации от несанкционированного доступа, имеющие действующий сертификат соответствия требованиям ФСТЭК, предъявляемым к средствам вычислительной техники не ниже 5 класса.

4.2.4 Регистрация событий безопасности (РСБ)

В подсистеме должны обеспечиваться:

15) определение событий безопасности, подлежащих регистрации, и сроков их хранения (РСБ.1);

16) определение состава и содержания информации о событиях безопасности, подлежащих регистрации (РСБ.2);

17) сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения (РСБ.3);

18) защита информации о событиях безопасности (РСБ.7).

Для реализации подсистемы должны использоваться:

– организационные меры защиты информации;

– средства защиты информации от несанкционированного доступа, имеющие действующий сертификат соответствия требованиям ФСТЭК, предъявляемым к средствам вычислительной техники не ниже 5 класса;

– средства межсетевого экранирования, имеющие действующий сертификат соответствия требованиям ФСТЭК (ФСБ), предъявляемым к межсетевым экранам не ниже 5 класса.

4.2.5 Подсистема антивирусной защиты (АВЗ)

В подсистеме должны обеспечиваться:

19) реализация антивирусной защиты (АВЗ.1);

20) обновление базы данных признаков вредоносных компьютерных программ (вирусов) (АВЗ.2).

Для реализации подсистемы должны использоваться:

– организационные меры защиты информации;

– средства антивирусной защиты информации, имеющие действующий сертификат соответствия требованиям ФСТЭК, предъявляемым к средствам антивирусной защиты не ниже 5 класса.

4.2.6 Подсистема анализа защищенности информации (АНЗ)

В подсистеме должны обеспечиваться:

21) контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации (АНЗ.2);

Для реализации подсистемы должны использоваться:

– организационные меры защиты информации;

– средства анализа защищенности, имеющие действующий сертификат соответствия требованиям ФСТЭК, предъявляемым к сканерам уязвимостей.

4.2.7 Подсистема защиты технических средств (ЗТС)

В подсистеме должны обеспечиваться:

22) организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования (ЗТС.2);

23) контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены (ЗТС.3);

24) размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр (ЗТС.4).

Для реализации подсистемы должны использоваться:

– организационные меры защиты информации.

4.2.8 Подсистема защиты информационной системы, ее средств, систем связи и передачи данных (ЗИС)

В подсистеме должны обеспечиваться:

25) обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи (ЗИС.3);

Для реализации подсистемы должны использоваться:

– организационные меры защиты информации;

– средства межсетевого экранирования, имеющие действующий сертификат соответствия требованиям ФСТЭК, предъявляемым к межсетевым экранам не ниже 4 класса;

– средства защиты каналов передачи данных, имеющие действующий сертификат соответствия требованиям ФСБ, предъявляемым к средствам криптографической защиты информации.

4.2 Требования к видам обеспечения

4.3.1 Требования к программному обеспечению

4.3.1.1 Выбор программных средств защиты должен проводиться с учетом средств защиты, эксплуатируемых у заказчика.

4.3.1.2 Средства защиты информации, входящие в состав СЗПДн, должны быть сертифицированы на соответствие требованиям руководящих документов ФСТЭК и ФСБ России.

4.3.1.3 При создании СЗПДн должно использоваться только лицензионное общее и специальное программное обеспечение и операционные системы.

4.3.1.4 Требования к программному обеспечению, используемому для защиты информации в ИСПДн «Сотрудники» (средств защиты информации, в том числе и встроенных в общесистемное и прикладное ПО) в части необходимости обеспечения контроля отсутствия в нем недекларированных возможностей (НДВ) должны быть определены в ТЗ.

4.3.2 Требования к техническому обеспечению

Выбор аппаратных (программно-аппаратных) средств защиты должен проводиться с учетом средств защиты, эксплуатируемых у заказчика.

4.3.3 Требования к организационному обеспечению

4.3.3.1 Мониторы АРМ должны располагаться таким образом, чтобы препятствовать возможности несанкционированного визуального съема информации с них.

4.3.3.2 Должна осуществляться физическая охрана устройств и носителей информации ИСПДн «Сотрудники», предусматривающая:

4.3.3.3 контроль доступа в помещения ИСПДн «Сотрудники» посторонних лиц;

4.3.3.4 наличие надежных препятствий для несанкционированного проникновения в помещение ИСПДн «Сотрудники» и хранилище носителей информации, особенно в нерабочее время.

4.3.3.5 Должны быть проведены работы по подготовке проектов и введению в действие следующих организационно-распорядительных документов, направленных на обеспечение информационной безопасности:

– приказов о назначении ответственных лиц;

– документа, определяющего политику в отношении обработки персональных данных;

– локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений;

– уведомления уполномоченного органа по защите прав субъектов персональных данных о намерении осуществлять обработку персональных данных;

– документов, определяющих круг лиц, имеющих доступ к ИСПДн, ее компонентам;

– форм согласия субъекта персональных данных на обработку его персональных данных;

– документа, содержащего перечень обрабатываемых персональных данных;

– документа, содержащего перечень нормативных правовых актов, в соответствии с которыми производится обработка персональных данных.

5 СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ СЗПДН

5.1 Проектирование СЗПДн, поставка оборудования, монтаж оборудования

5.1.1 Проектирование СЗПДн

Проводится обследование ИСПДн:

а) уточняется перечень ПДн, подлежащих защите;

б) уточняется информация о категориях и составе ПДн, обрабатываемых автоматизированными и неавтоматизированными способами;

в) проводится анализ состава ПДн в ИСПДн, собирается информация о защищенности ПДн;

г) уточняются условия расположения объекта защиты относительно границ контролируемой зоны;

д) уточняются конфигурация и топология ИСПДн и систем связи в целом и их компонентов, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;

е) уточняются состав технических средств и систем, предполагаемых к использованию в СЗПДн, условия их расположения, общесистемные и прикладные программные средства;

ж) уточняются режимы обработки информации в ИСПДн в целом и в отдельных ее компонентах;

з) для ИСПДн производится анализ собранной информации об угрозах и их показателях для разработки Модели угроз;

и) уточняется уровень защищенности ПДн, обрабатываемых в ИСПДн;

к) разрабатывается Модель угроз для ИСПДн на основе методических рекомендаций ФСТЭК России;

л) уточняется степень участия сотрудников в обработке информации, характер их взаимодействия между собой и со службой ИБ.

Также на данном этапе разрабатывается пакет организационно-распорядительной документации на ИСПДн.

6 ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ

6.1. Содержание отчетных материалов согласуется на уровне специалистов заказчика и исполнителя в соответствии с договором. Исполнитель должен быть заранее проинформирован заказчиком о порядке и сроках согласования отчетных материалов, перечне вопросов, которые подлежат согласованию, составе согласующих подразделений и организаций и степени их компетенции при согласовании тех или иных разделов отчетной документации.

6.3 В случае необходимости может быть проведена защита предлагаемых решений в процессе технического совещания специалистов исполнителя и заказчика.

6.4 Настоящее ТЗ может быть уточнено или изменено в процессе работы. Уточнения и изменения ТЗ производятся по согласованию сторон. Оформление изменений осуществляется выпуском дополнений, которые являются неотъемлемой частью настоящего ТЗ.

6.5 Согласование и утверждение изменений производится в том же порядке и теми же должностными лицами, что и согласование и утверждение ТЗ.

6.6 Замечания по отчетным материалам должны быть представлены исполнителю с техническим обоснованием в письменной форме.

7 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

7.1 Комплект проектных материалов предоставляется заказчику по предварительной договоренности в электронном виде и (или) на твердой копии. Вся разрабатываемая проектная документация должна быть выполнена на русском языке.

ПРИЛОЖЕНИЕ В

УТВЕРЖДАЮ

Генеральный директор ООО «Трехгорный керамический завод»

_____Е.В. Горбатов

«____» _____ 2018 г.

ПЕРЕЧЕНЬ ПЕРСОНАЛЬНЫХ ДАННЫХ,
подлежащих защите в автоматизированной системе обработки персональных данных
АС «Сотрудники»

№	Тип персональных данных, подлежащих защите
1.	Фамилия, Имя, Отчество
2.	Паспортные данные
3.	Пол
4.	Дата рождения
5.	Место рождения
6.	Адрес регистрации
7.	Адрес проживания
8.	СНИЛС (№ страхового пенсионного свидетельства)
9.	Сведения об образовании
10.	Сведения о воинском учете
11.	Индивидуальный номер налогоплательщика
12.	Номер, дата трудового договора
13.	Табельный номер

Генеральный директор ООО «Трехгорный керамический завод» _____ Е.В. Горбатов

ПРИЛОЖЕНИЕ Г

УТВЕРЖДАЮ

Генеральный директор ООО «Трехгорный керамический завод»

_____ В.Ю. Горбатов

«____» _____ 2018 г.

ИНСТРУКЦИЯ
ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ
в автоматизированной системе обработки персональных данных
АС «Сотрудники»

2018 г.

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данная инструкция определяет требования к организации защиты информационной системы (далее – ИС) Общества с ограниченной ответственностью «Трехгорный керамический завод» (далее – ООО «ТКЗ») от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения (далее – вредоносное ПО), устанавливает ответственность пользователей ИС, ответственного за обеспечение безопасности информации и других должностных лиц, за выполнение указанных требований.

II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. **Антивирусная база** – это база, которая содержит уникальные данные о каждом конкретном вирусе

2.2. **Антивирусная защита** – комплекс мер, направленных на предотвращение, обнаружение и обезвреживание действий вредоносного ПО при помощи антивирусных программных продуктов.

2.3. **Средство антивирусной защиты** – программный пакет, предназначенный для эффективной защиты, перехвата и удаления из операционной системы компьютера максимального количества вредоносных (или потенциально вредоносных) программ.

2.4. **Автоматизированное рабочее место (АРМ)** – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.

2.5. **Информационная система (ИС)** – система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию.

2.6. **Носитель информации** – любой материальный объект или среда, используемый для хранения или передачи информации

2.7. **Программное обеспечение** – все или часть программ, процедур, правил и соответствующей документации системы обработки информации (ISO/IEC 2382-1:1993)

2.8. **Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

III. ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

3.1. К использованию в ООО «ТКЗ» допускаются только сертифицированные и лицензионные средства антивирусной защиты, закупленные у разработчиков или поставщиков данных средств.

3.2. Установка средств антивирусного контроля на автоматизированных рабочих местах (далее – АРМ) и серверах ИС ООО «ТКЗ» осуществляется ответственным за обеспечение безопасности информации или под его контролем, настройка параметров средств антивирусного контроля осуществляется в соответствии с руководствами по применению конкретных антивирусных средств и требованиями нормативных документов ФСТЭК РФ в области защиты информации.

3.3. Антивирусный контроль должен быть настроен в режиме постоянной антивирусной защиты.

3.4. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), хранящаяся на АРМ, передающаяся по сети, а также информация на съемных носителях. Контроль входящей информации должен осуществляться автоматически, непосредственно после её приёма. При передаче файлов, запакованных в архивы, без их распаковки, должна вручную инициироваться антивирусная проверка этих архивов.

3.5. Процедура обновления баз средства антивирусной защиты должна проводиться в автоматическом режиме не реже 1 (одного) раза в день на всех АРМ ИС, работающих в сети, не реже 1 (одного) раза в неделю для всех АРМ ИС, работающих автономно.

3.6. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено ответственным за обеспечение безопасности информации на предмет отсутствия вредоносного программного обеспечения (далее – ПО).

3.7. Подключаемые к компьютеру внешние устройства и носители информации должны проверяться антивирусным ПО непосредственно после подключения.

3.8. Периодический контроль за состоянием антивирусной защиты (обновление антивирусной программы и антивирусных баз, а также проверка работоспособности средств антивирусной защиты) в ИС ООО «ТКЗ», осуществляется ответственным за обеспечение безопасности информации, пользователями ИС и всеми должностными лицами, настраивающими и сопровождающими средства антивирусной защиты в ИС ООО «ТКЗ».

IV. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ ИС

4.1. При возникновении подозрения на наличие вредоносного программного обеспечения (частые ошибки в работе программ, появление посторонних графических и звуковых эффектов, искажения данных, неконтролируемое пропадание файлов, появление сообщений о системных ошибках, замедление работы компьютера и т.п.) самостоятельно или вместе с ответственным за обеспечение безопасности информации провести внеочередной антивирусный контроль своего АРМ. При самостоятельном проведении антивирусного контроля - уведомить о результатах ответственного за обеспечение безопасности информации для определения им факта наличия или отсутствия вредоносного программного обеспечения.

4.2. В случае появления информационного окна средства антивирусной защиты, сигнализирующем об обнаружении вредоносного программного обеспечения:

4.2.1. приостановить обработку данных;

4.2.2. немедленно поставить в известность о факте обнаружения вредоносного программного обеспечения ответственного за обеспечение безопасности информации, владельца заражённых файлов, а также смежные структурные подразделения, использующие эти файлы в работе;

4.2.3. совместно с владельцем файлов, заражённых вредоносным программным обеспечением, провести анализ необходимости дальнейшего их использования;

4.2.4. произвести лечение или уничтожение заражённых файлов (при необходимости для выполнения требований данного пункта привлечь ответственного за обеспечение безопасности информации).

V. ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЯ ИС И ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ

5.1. Администратор и пользователи ИС несут персональную ответственность за соблюдение требований настоящей Инструкции, за качество проводимых им работ по обеспечению безопасности персональных данных и за все действия, совершенные от имени их учётных записей в ИС, если с их стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

5.2. Администратор и пользователи ИС при нарушении норм, регулирующих получение, обработку и защиту информации, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

5.3. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим сотрудникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами (приказами, распоряжениями) ООО «ТКЗ», влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Сотрудник ООО «ТКЗ», имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба ООО «ТКЗ» (в соответствии с п.7 ст. 243 Трудового кодекса РФ).

5.3.1. В отдельных случаях, при разглашении персональных данных, сотрудник, совершивший указанный проступок, несет ответственность в соответствии со статьей 13.14 Кодекса об административных правонарушениях РФ.

5.4. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса РФ.

Начальник технического отдела _____ Е.О. Федорчук

С инструкцией ознакомлены:

№	ФИО	Подпись
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		

ПРИЛОЖЕНИЕ Д

УТВЕРЖДАЮ

Генеральный директор ООО «Трехгорный керамический завод»

_____ В.Ю. Горбатов

«____» _____ 2018 г.

ИНСТРУКЦИЯ
ПО ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ
в автоматизированной системе обработки персональных данных
АС «Сотрудники»

2018 г.

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данная инструкция регламентирует процессы генерации, смены и прекращения действия паролей (удаления учётных записей пользователей) в информационных системах (далее – ИС) Общества с ограниченной ответственностью «Трехгорный керамический завод» (далее – ООО «ТКЗ»), а также контроль над действиями пользователей при работе с паролями.

1.2. Осуществление процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИС и контроль за действиями пользователей при работе с паролями возлагается на ответственного за обеспечение безопасности информации.

II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. **Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

2.2. **Информационная система (ИС)** – система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию.

2.3. **Пароль** – секретная комбинация цифр, знаков, слов, или осмысленное предложение, служащие для защиты информации от несанкционированного доступа к информационным ресурсам.

2.4. **Пользователь** – сотрудник, участвующий в рамках своих функциональных обязанностей в процессах обработки персональных данных.

2.5. **Компрометация пароля** – раскрытие, обнаружение или утеря пароля.

III. ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

3.1. Правила формирования паролей:

3.1.1. Личные пароли должны генерироваться и распределяться централизованно, либо выбираться пользователями информационной системы самостоятельно с учетом следующих требований:

3.1.1.1. длина пароля должна быть не менее 6 символов;

3.1.1.2. в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

3.1.1.3. пароль не должен включать в себя имя пользователя, легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, абвгд и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе.

3.1.1.4. при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6-ти позициях;

3.1.2. Пользователям допускается использовать пароли, составленные из первых букв слов запоминающихся высказываний в разном регистре, смешанные в произвольном порядке со специальными символами.

3.1.3. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на ответственного за обеспечение безопасности информации.

3.2. Порядок смены личных паролей:

3.2.1. Смена паролей должна проводиться регулярно, не реже одного раза в 3 месяца.

3.2.2. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т.п.) должно производиться немедленное удаление его учётной записи сразу после окончания последнего сеанса работы данного пользователя с системой.

3.2.3. Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) ответственных за обеспечение безопасности информации, администраторов информационной системы и других сотрудников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

3.2.4. Ответственный за обеспечение безопасности информации ведёт «Журнал учёта работ в информационных системах», в котором он отмечает факт смены паролей пользователей.

3.2.4.1. Временный пароль, заданный ответственным за обеспечение безопасности информации при регистрации нового пользователя, должен действовать в течение ограниченного срока времени. Пользователь должен изменить временный пароль при первом входе в систему.

3.3. Действия в случае утери и компрометации пароля:

3.3.1. В случае утери или компрометации (разглашения, утраты) или подозрения в компрометации пароля пользователя должна быть немедленно проведена внеплановая процедура смены пароля.

IV. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ ИС

4.1. Правила формирования паролей:

4.1.1. Личные пароли должны генерироваться и распределяться централизованно, либо выбираться пользователями информационной системы самостоятельно с учетом следующих требований:

4.1.1.1. длина пароля должна быть не менее 6 символов;

4.1.1.2. в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

4.1.1.3. пароль не должен включать в себя имя пользователя, легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, абвгд и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе;

4.1.1.4. при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6-ти позициях.

4.1.2. Сотрудникам допускается использовать пароли, составленные из первых букв слов запоминающихся высказываний в разном регистре, смешанные в произвольном порядке со специальными символами.

4.1.3. Для обеспечения возможности использования имён и паролей некоторых сотрудников в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.), сотрудники обязаны сразу же после установки своих паролей передавать их на хранение вместе с именами своих учетных записей ответственному за обеспечение безопасности информации в запечатанном конверте или опечатанном пенале.

4.2. Порядок Ввод пароля:

4.2.1. При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или в отраженном свете) и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.).

4.3. Порядок смены личных паролей:

4.3.1. Смена паролей должна проводиться регулярно, не реже одного раза в 3 месяца, самостоятельно каждым пользователем.

4.3.2. Временный пароль, заданный ответственным за обеспечение безопасности информации при регистрации нового пользователя, должен действовать в течение ограниченного срока времени. Пользователь должен изменить временный пароль при первом входе в систему.

4.4. Хранение пароля:

4.4.1. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке, мобильном телефоне и любых других предметах и носителях информации.

4.4.2. Запрещается сообщать свой пароль полностью или частично другим пользователям, запрещается спрашивать или подсматривать пароль других пользователей.

4.4.3. Запрещается регистрировать других пользователей в ИС со своим личным паролем, запрещается входить в ИС под учётной записью и паролем другого пользователя.

4.5. Действия в случае утери и компрометации пароля:

4.5.1. В случае утери или компрометации (разглашения, утраты) или подозрения в компрометации пароля пользователь должен немедленно обратиться к ответственному за обеспечение безопасности информации с целью смены личного пароля.

V. ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЯ ИС И ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ

5.1. Администратор и пользователи ИС несут персональную ответственность за соблюдение требований настоящей Инструкции, за качество проводимых ими работ по обеспечению безопасности информации и за все действия, совершенные от имени их учётных записей в ИС, если с их стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

5.2. Администратор и пользователи ИС при нарушении норм, регулирующих получение, обработку и защиту информации, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

5.3. Разглашение информации (передача их посторонним лицам, в том числе другим сотрудникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами (приказами, распоряжениями) ООО «ТКЗ», влечет наложение на сотрудника, имеющего доступ к защищаемой информации, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Сотрудник ООО «ТКЗ», имеющий доступ к информации и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба ООО «ТКЗ» (в соответствии с п.7 ст. 243 Трудового кодекса РФ).

5.3.1. В отдельных случаях, при разглашении персональных данных, сотрудник, совершивший указанный проступок, несет ответственность в соответствии со статьей 13.14 Кодекса об административных правонарушениях РФ.

5.4. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса РФ.

Начальник технического отдела _____ Е.О. Федорчук

ПРИЛОЖЕНИЕ Е

УТВЕРЖДАЮ

Генеральный директор ООО «Трехгорный керамический завод»

_____ В.Ю. Горбатов

«____» _____ 2018 г.

ИНСТРУКЦИЯ
АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

в автоматизированной системе обработки персональных данных
АС «Сотрудники»

2018 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данная Инструкция определяет основные обязанности и права администратора безопасности информационных систем персональных данных (далее – ИСПДн) Общества с ограниченной ответственностью «Трехгорный керамический завод» (далее – ООО «ТКЗ»).

1.2. Администратор безопасности ИСПДн является штатным сотрудником ООО «ТКЗ».

1.3. Администратор безопасности ИСПДн назначается приказом руководителя ООО «ТКЗ».

1.4. Решение вопросов обеспечения информационной безопасности входит в прямые служебные обязанности администратора безопасности ИСПДн.

1.5. Администратор безопасности ИСПДн обладает правами доступа к любым программным и аппаратным ресурсам ИСПДн.

1.6. Администратор безопасности должен иметь специальное рабочее место – рабочую станцию (РС), размещенную в отдельном помещении и функционирующую постоянно при включении сети.

2. ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ

Администратор безопасности ИСПДн обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Знать перечень установленных в подразделениях ООО «ТКЗ» автоматизированных рабочих мест (далее АРМ) и перечень задач, решаемых с их использованием.

2.3. Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн:

программного обеспечения АРМ (операционные системы, прикладное и специальное ПО);

аппаратных средств;

аппаратных и программных средств защиты.

2.4. Обеспечивать функционирование и поддерживать работоспособность элементов ИСПДн, в том числе средств защиты информации, и локальной вычислительной сети.

2.5. Информировать ответственного за обеспечение защиты персональных данных о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

2.6. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.

2.7. Хранить, осуществлять прием и выдачу персональных паролей пользователей, осуществлять контроль за правильностью использования персонального пароля.

2.8. Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.

2.9. В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.10. Осуществлять учет и периодический контроль за составом и полномочиями пользователей различных АРМ (далее – ИСПДн).

2.11. Осуществлять оперативный контроль за работой пользователей защищенных АРМ, анализировать содержимое системных журналов всех АРМ и адекватно реагировать на возникающие нештатные ситуации. Обеспечивать своевременное архивирование системных журналов АРМ и надлежащий режим хранения данных архивов.

2.12. Осуществлять непосредственное управление режимами работы и административную поддержку функционирования применяемых на АРМ ИСПДн специальных технических средств защиты от несанкционированного доступа (далее – НСД).

2.13. Присутствовать при внесении изменений в конфигурацию (модификации) аппаратно-программных средств защищенных АРМ сторонними физическими лицами и организациями.

2.14. Периодически проверять состояние используемых средств защиты информации (далее – СЗИ) от НСД, осуществлять проверку правильности их настройки (выборочное тестирование).

2.15. Периодически контролировать целостность печатей (пломб, наклеек) на устройствах защищенных АРМ.

2.16. Проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИС и осуществления НСД к информации и техническим средствам АРМ.

2.17. По указанию руководства своевременно и точно отражать изменения в организационно-распорядительных и нормативных документах по управлению средствами защиты от НСД, установленных на АРМ ИСПДн.

2.18. Проводить занятия с сотрудниками по правилам работы на АРМ, оснащенных СЗИ от НСД, и по изучению руководящих документов по вопросам обеспечения безопасности информации.

2.19. Участвовать в расследовании причин совершения нарушений и возникновения серьезных кризисных ситуаций в результате НСД.

2.20. Участвовать в работе комиссий по пересмотру планов защиты.

3. ПОРЯДОК РАБОТЫ С РЕСУРСАМИ ИСПДН

Перечень работ, производимых администратором безопасности ИСПДн.

3.1. Проверка работоспособности и настройка системы доступа к ресурсам ИСПДн:

3.1.1. администратор безопасности ИСПДн разрабатывает правила парольной защиты и контролирует их соблюдение;

3.1.2. администратор безопасности ИСПДн сообщает пользователю его уникальное имя и предоставляет возможность задать пароль, кодирует аппаратный идентификатор пользователя (при наличии);

3.1.3. администратор безопасности ИСПДн производит изменения учетных данных пользователя по требованию ответственного за обеспечение безопасности персональных данных, а также периодически по утвержденному плану и в случае увольнения сотрудника;

3.1.4. администратор безопасности ИСПДн имеет право в целях тестирования уязвимости системы доступа (выявление простейших паролей) производить попытки взлома паролей пользователей, в случае успешного взлома, администратор безопасности ИСПДн обязан потребовать у пользователя изменения пароля.

3.2. Проверка работоспособности и настройка аппаратных и программных средств защиты информации:

3.2.1. администратор безопасности ИСПДн обязан перед началом работ включить и убедиться в работоспособности аппаратных СЗИ, в случае сбоя – прекратить работы.

3.2.2. в случае сбоя программных СЗИ, таких, как неправильная идентификация и аутентификация пользователей, администратор безопасности ИСПДн обязан прекратить работы, в случае производственной необходимости продолжения работ – отключить программное обеспечение (далее – ПО) СЗИ и лично контролировать проведение работ пользователем.

3.3. Антивирусная защита ресурсов ИСПДн:

3.3.1. администратор безопасности ИСПДн в соответствии с инструкцией по организации антивирусной защиты разрабатывает и контролирует реализацию антивирусной политики, а именно:

– настраивает параметры антивирусной программы;

– контролирует работоспособность антивирусной программы;

– немедленно реагирует на сообщения пользователей о подозрительном поведении ПО, а также о появлении любых сообщений антивирусной программы;

– имеет право на проведение внеплановой проверки на присутствие вирусов;

– периодически обновляет антивирусные базы данных, а также исполняемые модули антивирусной программы.

3.4. Хранение дистрибутивов программного обеспечения СЗИ:

3.4.1. администратор безопасности ИСПДн должен хранить дистрибутивы ПО СЗИ, установленных на АРМ ИСПДн, в месте, исключающем доступ посторонних лиц.

3.5. Проверка целостности системного и прикладного ПО:

3.5.1. администратор безопасности ИСПДн должен периодически (не реже одного раза в квартал) производить проверку целостности системного и прикладного программного обеспечения с использованием специальных режимов работы СЗИ от НСД.

3.6. Вывод ресурсов ИС из эксплуатации:

3.6.1. при невозможности ремонта технических средств ИСПДн администратор безопасности ИСПДн обязан:

– физически уничтожать любые носители, независимо от содержащейся на них информации, отразить факт уничтожения носителя в «Журнале учета машинных носителей персональных данных»;

– отразить факт выхода из строя и замены оборудования в «Техническом паспорте ИСПДн».

4. ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

4.1. К попыткам несанкционированного доступа относятся:

4.1.1. сеансы работы с ИСПДн незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, либо срок действия полномочий которых истек, либо в состав полномочий которых не входят реализуемые в процессе сеанса работы операции;

4.1.2. действия третьего лица, пытающегося получить доступ (или получившего доступ) к ИСПДн, при использовании учетной записи администратора или другого пользователя ИСПДн, в целях получения коммерческой или другой личной выгоды, методом подбора пароля или другого метода (случайного разглашения пароля и т.п.) без ведома владельца учетной записи.

4.2. При выявлении факта НСД администратор безопасности ИСПДн обязан:

4.2.1. прекратить доступ к ИСПДн со стороны выявленного участка НСД;

4.2.2. доложить руководителю ООО «ТКЗ» служебной запиской о факте НСД, его результате (успешный, неуспешный) и предпринятых действиях;

4.2.3. известить ответственного за обеспечение безопасности персональных данных и начальника отдела, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка НСД, о факте НСД;

4.2.4. проанализировать характер НСД, по результатам анализа составить письменный отчет и предоставить его руководителю ООО «ТКЗ».

5. ПРАВА

5.1. Администратор безопасности ИСПДн имеет право:

5.1.1. требовать от пользователей информационных ресурсов выполнения инструкций пользователя ИСПДн;

5.1.2. проводить служебные расследования по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн;

5.1.3. вносить свои предложения по совершенствованию мер защиты в ИСПДн.

6. ОТВЕТСТВЕННОСТЬ

6.1. Администратор безопасности ИСПДн несет ответственность за соблюдение требований настоящей инструкции, а также других нормативных документов в области защиты информации.

6.2. Администратор безопасности ИСПДн несет ответственность за программно-аппаратные, инженерно-технические и криптографические средства защиты информации, средства вычислительной техники, информационно - вычислительные комплексы, сети и информационные системы обработки информации, закрепленные за ним приказом руководителя ООО «ТКЗ» и за качество проводимых им работ по обеспечению защиты информации в соответствии с функциональными обязанностями.

6.3. Администратор безопасности ИСПДн несет ответственность по действующему законодательству за разглашение информации, составляющей персональные данные, ставшие известными ему по роду работы.

6.4. Администратор безопасности ИСПДн несет ответственность за все действия, совершенные от имени его учетной записи или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

Начальник технического отдела _____ Е.О. Федорчук

ПРИЛОЖЕНИЕ Ж

УТВЕРЖДАЮ

Генеральный директор ООО «Трехгорный керамический завод»

_____ В.Ю. Горбатов

«____» _____ 2018 г.

ИНСТРУКЦИЯ
ПОЛЬЗОВАТЕЛЯ ИС
в автоматизированной системе обработки персональных данных
АС «Сотрудники»

2018 г.

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция регламентирует обязанности сотрудников, участвующих в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющих доступ к аппаратным средствам, программному обеспечению и данным информационной системы (далее ИС) общества с ограниченной ответственностью (далее – ООО «ТКЗ»).

II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. **Автоматизированное рабочее место (АРМ)** – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.

2.2. **База данных** – это информация, упорядоченная в виде набора элементов, записей одинаковой структуры

2.3. **Информационная система (ИС)** – система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию.

2.4. **Носитель информации** – любой материальный объект или среда, используемый для хранения или передачи информации.

2.5. **Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

2.6. **Программное обеспечение** – все или часть программ, процедур, правил и соответствующей документации системы обработки информации (ISO/IEC 2382-1:1993)

2.7. **Средство защиты информации (СЗИ)** – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

III. ОБЩИЕ ОБЯЗАННОСТИ СОТРУДНИКОВ

Каждый сотрудник ООО «ТКЗ», являющийся пользователем ИС, обязан:

3.1. Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИС.

3.2. Знать и строго выполнять правила работы со средствами защиты информации, установленными на его автоматизированном рабочем месте (далее АРМ).

3.3. Соблюдать правила работы с паролем своей учётной записи.

3.4. Немедленно вызывать ответственного за обеспечение безопасности информации и поставить в известность руководителя структурного подразделения при обнаружении:

3.4.1. нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа к защищаемой АРМ;

3.4.2. несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ;

3.4.3. отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;

3.4.4. некорректного функционирования установленных на АРМ технических средств защиты;

3.4.5. непредусмотренных отводов кабелей и подключенных к АРМ дополнительных устройств.

3.5. Всем сотрудникам ООО «ТКЗ», являющимся пользователями ИС, запрещается:

3.5.1. использовать компоненты программного и аппаратного обеспечения ИС ООО «ТКЗ» в неслужебных целях;

3.5.2. самовольно вносить какие-либо изменения в конфигурацию АРМ или устанавливать в АРМ любые программные и аппаратные средства, кроме выданных или разрешённых к использованию ответственным за обеспечение безопасности персональных данных;

3.5.3. оставлять без присмотра своё АРМ не активизировав блокировки доступа или оставлять своё АРМ включенным по окончании работы;

3.5.4. умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушению безопасности персональных данных.

IV. ОБЕСПЕЧЕНИЕ СОХРАННОСТИ ИНФОРМАЦИИ

4.1. Для обеспечения сохранности электронных информационных ресурсов ООО «ТКЗ» необходимо соблюдать следующие требования:

4.1.1. Для копирования информации не должны использоваться непроверенные на наличие компьютерных вирусов и других вредоносных программ носители информации.

4.2. Субъектам доступа запрещается:

4.2.1. Установка и использование при работе в АРМ вредоносных программ, ведущих к блокированию работы сети.

4.2.2. Самовольное изменение сетевых адресов.

4.2.3. Самовольное вскрытие блоков АРМ, модернизация или модификация АРМ и программного обеспечения.

4.2.4. Несанкционированная передача АРМ с прописанными сетевыми настройками. Передача АРМ из одного подразделения в другое производится только ответственным за обеспечение безопасности информации с предварительно удаленными сетевыми настройками.

4.2.5. Использование технологии беспроводного доступа без разрешения Ответственного за обеспечение безопасности в информационных системах.

4.3. Сведения, содержащиеся в электронных документах и базах данных ООО «ТКЗ», должны использоваться только в служебных целях в рамках полномочий сотрудника, работающего с соответствующими материалами.

V. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ПРАВИЛ РАБОТЫ

5.1. Каждый пользователь ИС несёт персональную ответственность за соблюдение требований настоящей Инструкции и за все действия, совершенные от имени его учётной записи в ИС, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

5.2. За разглашение персональных данных и нарушение порядка работы со средствами ИС, содержащими персональные данные, сотрудники могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.

5.3. Распространение персональных данных субъекта (передача их посторонним лицам, в том числе другим сотрудникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами (приказами, распоряжениями) ООО «ТКЗ», влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Сотрудник ООО «ТКЗ», имеющий доступ к персональным данным субъекта

5.4. и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба ООО «ТКЗ» (в соответствии с п.7 ст. 243 Трудового кодекса РФ).

5.4.1. В отдельных случаях, при разглашении персональных данных, сотрудник, совершивший указанный проступок, несет ответственность в соответствии со статьей 13.14 Кодекса об административных правонарушениях РФ.

5.5. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса РФ.

Начальник технического отдела _____ Е.О. Федорчук

ПРИЛОЖЕНИЕ З

УТВЕРЖДАЮ

Генеральный директор ООО «Трехгорный керамический завод»

_____ В.Ю. Горбатов

«____» _____ 2018 г.

ИНСТРУКЦИЯ
ПО ЭКСПЛУАТАЦИИ СЗИ
в автоматизированной системе обработки персональных данных
АС «Сотрудники»

2018 г.

1. Общие положения

Настоящая Инструкция по эксплуатации средств защиты информации в информационной системе «Сотрудники» (далее – Инструкция) разработана для пользователей и администратора безопасности информации (далее – ИС) и определяет правила эксплуатации средств защиты информации, установленных в информационной системе «Сотрудники» (далее – ИС), а также устанавливает ответственность пользователей ИС за их нарушение.

2. Правила эксплуатации средств защиты информации

2.1. Для обеспечения необходимого уровня защищенности при работе в ИС применяются следующие средства защиты информации:

– Средство защиты информации от несанкционированного доступа «Dallas Lock 8.0-K»;

– Программный комплекс «ViPNet Client 4.0»;

– Средство антивирусной защиты Kaspersky Endpoint Security версия 10.

2.2. Эксплуатация средств защиты информации осуществляется в соответствии с эксплуатационной документацией, предоставляемой производителями средств защиты информации.

2.3. Пользователи ИС должны быть ознакомлены со следующими документами:

– Система защиты информации от несанкционированного доступа Dallas Lock 8.0. Руководство оператора. RU.48957919.501410-01 34;

– ViPNet Контроль приложений 4.0. Руководство пользователя. ФРКЕ. 00004-05 34 04;

– Основные термины и определения. Приложение к документации ViPNet CUSTOM. ФРКЕ. 00068-02 90 02;

– Kaspersky Endpoint Security версия 10. Руководство пользователя.

2.4. Администратор безопасности информации при эксплуатации средств защиты информации должен руководствоваться следующими документами:

– Система защиты информации от несанкционированного доступа Dallas Lock 8.0. Руководство по эксплуатации. RU.48957919.501410-02 92;

– Система защиты информации от несанкционированного доступа Dallas Lock 8.0. Руководство оператора. RU.48957919.501410-01 34;

– Система защиты информации от несанкционированного доступа Dallas Lock 8.0. Описание применения. RU.48957919.501410-01 31;

– ViPNet Контроль приложений 4.0. Руководство пользователя. ФРКЕ. 00004-05 34 04;

– Основные термины и определения. Приложение к документации ViPNet CUSTOM. ФРКЕ. 00068-02 90 02;

– Kaspersky Endpoint Security 10. Руководство пользователя.

2.5. Пользователи ИС должны быть ознакомлены с организационно-распорядительными документами ООО «Трехгорный керамический завод» по защите информации в ИС.

2.6. Перед началом эксплуатации средств защиты информации администратором безопасности информации должен быть проведен контроль знаний и навыков пользователей ИС в части обеспечения безопасности информации с использованием применяемых в ИС средств защиты информации.

2.7. Внесение изменений в конфигурацию используемых средств защиты информации осуществляет администратор безопасности информации после согласия с ответственным за обеспечение безопасности персональных данных.

2.8. Администратор безопасности информации должен периодически проводить плановые и внеплановые проверки выполнения пользователями ИС требований по защите информации в ИС.

2.9. Администратором безопасности информации осуществляется контроль работоспособности, параметров настройки и правильности функционирования средств защиты информации один раз в полгода, а также в случае изменения списка допущенных лиц, смены администратора безопасности информации, изменения конфигурации ИС.

3. Ответственность

Пользователи и администратор безопасности информации ИС несут персональную ответственность за нарушение правил эксплуатации средств защиты информации.

Начальник технического отдела _____ Е.О. Федорчук

ПРИЛОЖЕНИЕ И

УТВЕРЖДЕНА
приказом
Ген. директора
ООО «Трехгорный
керамический завод»
От _____ № __ ___

ЖУРНАЛ

учета машинных носителей информации ООО «Трехгорный керамический завод»

Начат:	
Окончен:	
Количество листов:	
Срок хранения:	**5 лет**

№ п/п	Регистрационный (учетный номер) или маркировка носителя	Тип носителя и его емкость	Модель носителя	Дата поступления	Отметка о получении (Ф.И.О.,подпись, дата)	Отметка об обратном приеме (Ф.И.О.,подпись, дата)	Место хранния	Дата и номер акта уничтожения	Примечание

ПРИЛОЖЕНИЕ К

УТВЕРЖДАЮ

Генеральный директор ООО «Трехгорный керамический завод»

_____ В.Ю. Горбатов

«____» _____ 2018 г.

МОДЕЛЬ УГРОЗ

автоматизированной системы обработки персональных данных «Сотрудники»

2018 г.

1 **ВВЕДЕНИЕ**

Модель угроз и модель нарушителя безопасности персональных данных (далее – Модель угроз) при их обработке в ИСПДн «Сотрудники» строится на основании анализа ИСПДн.

В модели угроз представлено описание структуры ИСПДн, состава и режима обработки ПДн, классификации потенциальных нарушителей, оценку исходного уровня защищенности, анализ угроз безопасности персональных данных.

Анализ УБПДн включает:

- описание угроз;
- оценку вероятности возникновения угроз;
- оценку реализуемости угроз;
- оценку опасности угроз;
- определение актуальности угроз.

2 ОПИСАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1.1. Наименование ИСПДн

Наименование ИСПДн – «Сотрудники». ИСПДн является собственностью общества с ограниченной ответственностью «Трехгорный керамический завод» (далее – Оператор).

1.2. Назначение ИСПДн

ИСПДн «Сотрудники» предназначена для обработки персональных данных сотрудников общества с ограниченной ответственностью «Трехгорный керамический завод».

1.3. Местонахождение ИСПДн

Информационная система располагается по адресу: 456082, г. Трехгорный Челябинской области, ул. Заречная,1А, а/я 254.

1.4. Охрана помещений

В зданиях с ИСПДн установлена охранная и пожарная сигнализация.

1.5. Взаимодействие с другими ИС

Взаимодействие ИСПДн «Сотрудники» с другими информационными системами не предполагается.

1.6. Состав ПДн

В соответствии с Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» ИСПДн «Сотрудники» является информационной системой, обрабатывающей иные категории персональных данных менее чем 100000 субъектов, являющихся сотрудниками оператора.

1.7. Общая информация о среде функционирования СКЗИ

Рабочие станции пользователей и серверы функционируют под управлением операционных систем Microsoft Windows 7.

3 ОПРЕДЕЛЕНИЕ АКТУАЛЬНОСТИ ИСПОЛЬЗОВАНИЯ СКЗИ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Использование СКЗИ для обеспечения безопасности персональных данных необходимо в следующих случаях:

— если персональные данные подлежат криптографической защите в соответствии с законодательством Российской Федерации;

— если в информационной системе существуют угрозы, которые могут быть нейтрализованы только с помощью СКЗИ.

Кроме того, решение о необходимости криптографической защиты персональных данных может быть принято конкретным оператором на основании технико-экономического сравнения альтернативных вариантов обеспечения требуемых характеристик безопасности информации, содержащей, в том числе, персональные данные.

К случаям, когда угрозы могут быть нейтрализованы только с помощью СКЗИ, относятся:

— передача персональных данных по каналам связи, не защищенным от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий на эту информацию (например, при передаче персональных данных по информационно-телекоммуникационным сетям общего пользования);

— хранение персональных данных на носителях информации, несанкционированный доступ к которым со стороны нарушителя не может быть исключен с помощью некриптографических методов и способов.

Оператором осуществляется передача персональных данных по информационно-телекоммуникационным сетям общего пользования, следовательно, есть необходимость использования средств криптографической защиты информации.

4 КЛАССИФИКАЦИЯ НАРУШИТЕЛЕЙ

Анализ возможностей, которыми может обладать нарушитель, проводится в рамках модели нарушителя.

При разработке модели нарушителя зафиксированы следующие положения:

1) Безопасность ПДн в ИСПДн обеспечивается средствами защиты информации ИСПДн, а также используемыми в них информационными технологиями, техническими и программными средствами, удовлетворяющими требованиям по защите информации, устанавливаемым в соответствии с законодательством Российской Федерации;

2) Средства защиты информации (СЗИ) штатно функционируют совместно с техническими и программными средствами, которые способны повлиять на выполнение предъявляемых к СЗИ требований;

3) СЗИ не могут обеспечить защиту ПДн от действий, выполняемых в рамках предоставленных субъекту действий полномочий (например, СЗИ не может обеспечить защиту ПДн от раскрытия лицами, которым предоставлено право на доступ к этим данным).

4.1. Классификация нарушителей

С точки зрения наличия права постоянного или разового доступа в контролируемую зону объектов размещения ИСПДн все физические лица могут быть отнесены к следующим двум категориям:

— категория I – лица, не имеющие права доступа в контролируемую зону ИСПДн;

— категория II – лица, имеющие право доступа в контролируемую зону ИСПДн.

По признаку принадлежности к ИСПДн все нарушители делятся на две группы:

1) внешние нарушители – физические лица, осуществляющие целенаправленное деструктивное воздействие, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн (категория I);

2) внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн (категория II).

4.2. Внешний нарушитель

В качестве внешнего нарушителя информационной безопасности рассматривается нарушитель, который не имеет непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны.

Предполагается, что внешний нарушитель не может воздействовать на защищаемую информацию по техническим каналам утечки, так как объем информации, хранимой и обрабатываемой в ИСПДн, является недостаточным для возможной мотивации внешнего нарушителя к осуществлению действий, направленных на утечку информации по техническим каналам утечки.

Предполагается, что внешний нарушитель может воздействовать на защищаемую информацию только во время ее передачи по каналам связи, а также атаки на ИСПДн путем реализации угроз удаленного доступа.

4.3. Внутренний нарушитель

К такому виду нарушителя могут относиться:

1) пользователи ИСПДн, т.е. работники, имеющие право доступа к ИСПДн (категория I);

2) работники, не имеющие права доступа к ИСПДн (категория II);

3) администраторы ИСПДн (категория III);

4) разработчики и поставщики программно-технических средств, расходных материалов, услуг (категория IV).

Лица категории I (пользователи ИСПДн, т.е. работники, имеющие право доступа к ИСПДн) не могут являться внутренними нарушителями, т.к. работники принимаемые на должности прошли тщательный отбор и расстановку по должностям (отбор осуществляют профессионально обученные и отобранные работники). Также введены ограничения привилегированными пользователями (администраторами ИСПДн) для пользователей ИСПДн программными средствами. Работники ознакомлены под подпись с организационно-распорядительными документами и ответственностью за нарушения. Объем информации, хранимой и обрабатываемой в ИСПДн, является недостаточным для возможной мотивации.

Лица категории II (работники, не имеющие права доступа к ИСПДн) в виду действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, а также благодаря тщательно отобранным и расстановленным на должности кадрам (данный отбор осуществляют профессионально обученные и отобранные работники), не могут являться внутренними нарушителями.

Лица категорий III (администраторы ИСПДн) являются привилегированными пользователями информационной системы, которые назначаются из числа особо доверенных лиц и осуществляю техническое обслуживание технических и программных средств защиты информации, включая их настройку, конфигурирование и разграничение доступа другим пользователям, также хорошо знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах ИСПДн в целом, а также с применяемыми принципами и концепциями безопасности.

Предполагается, что лица категории III не могут являться внутренними нарушителями.

Лица категории IV (разработчики и поставщики программно-технических средств, расходных материалов, услуг) не могут являться внутренними нарушителями, так как все работы проводимые данными лицами в ИСПДн происходят под контролем администраторов ИСПДн или ответственных лиц. Свободный доступ в помещения ИСПДн данным лицам ограничен в виду реализации комплекса организационно-технических мер.

Возможности нарушителей существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, принятию на работу, назначению на должность и обеспечению высокой профессиональной подготовки кадров, контролю допуска физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированного доступа.

В силу этого, внутренний нарушитель не имеет возможности получения специальных знаний о ИСПДн в объеме, необходимом для решения вопросов создания и преодоления средств защиты ПДн, и исключается его возможность по созданию и применению специальных программно-технических средств реализации целенаправленных воздействий данного нарушителя на подлежащие защите объекты.

Возможность сговора внутренних нарушителей между собой, а также сговора внутреннего и внешнего нарушителей исключена.

Следовательно, внутреннего нарушителя как группу можно исключить из списка актуальных нарушителей.

4.4. Предположения об имеющейся у нарушителя информации об объектах реализации угроз

В качестве основных уровней знаний нарушителей об АС можно выделить следующие:

1) общая информация – информации о назначениях и общих характеристиках ИСПДн;

2) эксплуатационная информация – информация, полученная из эксплуатационной документации;

3) чувствительная информация – информация, дополняющая эксплуатационную информацию об ИСПДн (например, сведения из проектной документации ИСПДн).

В частности, нарушитель может иметь:

1) данные об организации работы, структуре и используемых технических, программных и программно-технических средствах ИСПДн;

2) сведения об информационных ресурсах ИСПДн: порядок и правила создания, хранения и передачи информации, структура и свойства информационных потоков;

3) данные об уязвимостях, включая данные о недокументированных (недекларированных) возможностях технических, программных и программно-технических средств ИСПДн;

4) данные о реализованных в ПСЗИ принципах и алгоритмах;

5) исходные тексты программного обеспечения ИСПДн;

6) сведения о возможных каналах реализации угроз;

7) информацию о способах реализации угроз.

Предполагается, что внешний нарушитель владеет только информацией о назначениях и общих характеристиках ИСПДн.

Степень информированности нарушителя зависит от многих факторов, включая реализованные конкретные организационные меры и компетенцию нарушителей. Поэтому объективно оценить объем знаний вероятного нарушителя в общем случае практически невозможно, но учитывая, что объем информации, хранимой и обрабатываемой в ИСПДн, является недостаточным для возможной мотивации высококвалифицированного нарушителя, можно предположить, что информированность внешнего нарушителя будет минимальной.

4.5. Предположения об имеющихся у нарушителя средствах реализации угроз

Предполагается, что внешний нарушитель имеет:

1) доступные в свободной продаже технические средства и программное обеспечение;

Вместе с тем предполагается, что внешний нарушитель не имеет:

1) специально разработанные технические средства и программное обеспечение;

2) аппаратные компоненты СЗПДн и СФ СЗПДн;

3) средств перехвата в технических каналах утечки;

4) средств воздействия через сигнальные цепи (информационные и управляющие интерфейсы СВТ);

5) средств воздействия на источники и через цепи питания;

6) средств воздействия через цепи заземления;

7) средств активного воздействия на технические средства (средств облучения).

5 ИСХОДНЫЙ УРОВЕНЬ ЗАЩИЩЕННОСТИ ИСПДН

Под общим уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн (Y1).

В таблице представлены характеристики уровня исходной защищенности для ИСПДн «Сотрудники».

Таблица №3 – Исходный уровень защищенности

№	Технические и эксплуатационные характеристики		Уровень защищенности
1	По территориальному размещению	Локальная ИСПДн, развернутая в пределах одного здания	Высокий
2	По наличию соединения с сетями общего пользования	ИСПДн, имеющая одноточечный выход в сеть общего пользования	Средний
3	По встроенным (легальным) операциям с записями баз персональных данных	Модификация, передача	Низкий
4	По разграничению доступа к персональным данным	ИСПДн, к которой имеет доступ определенный перечень работников организации, являющейся владельцем ИСПДн, либо субъект ПДн	Средний
5	По наличию соединений с другими базами ПДн иных ИСПДн	ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	Высокий
6	По уровню (обезличивания) ПДн	ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	Низкий
7	По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	ИСПДн, не предоставляющая никакой информации	Высокий

В соответствии с полученными данными устанавливается **средний показатель исходной защищенности**. Устанавливается значение коэффициента **Y1=5.**

6 ВЕРОЯТНОСТЬ РЕАЛИЗАЦИИ УБПДН

Под вероятностью реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИСПДн в складывающихся условиях обстановки.

Числовой коэффициент (Y2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

–**маловероятно** – отсутствуют объективные предпосылки для осуществления угрозы (Y2 = 0);

–**низкая вероятность** – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (Y2 = 2);

–**средняя вероятность** – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны (Y2 = 5);

–**высокая вероятность** – объективные предпосылки для реализации угрозы существуют, и меры по обеспечению безопасности ПДн не приняты (Y2 = 10).

7 РЕАЛИЗУЕМОСТЬ УГРОЗ

По итогам оценки уровня защищенности (Y1) и вероятности реализации угрозы (Y2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы. Коэффициент реализуемости угрозы Y будет определяться соотношением Y = (Y1 + Y2)/20.

- если **0 ≤ Y ≤ 0,3**, то возможность реализации угрозы признается низкой;
- если **0,3 < Y ≤ 0,6**, то возможность реализации угрозы признается средней;
- если **0,6 < Y ≤ 0,8**, то возможность реализации угрозы признается высокой;
- если **Y > 0,8**, то возможность реализации угрозы признается очень высокой.

8 ОЦЕНКА ОПАСНОСТИ УГРОЗ

Оценка опасности УБПДн производится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который имеет три значения:

–**низкая опасность** - если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

–**средняя опасность** - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

–**высокая опасность** - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

9 ОПРЕДЕЛЕНИЕ АКТУАЛЬНОСТИ УГРОЗ В ИСПДН

В соответствии с правилами отнесения угрозы безопасности к актуальной, для ИСПДн определяются актуальные и неактуальные угрозы.

Таблица №4 – Правила определения актуальности УБПДн

Возможность реализации угрозы	**Показатель опасности угрозы**		
	Низкая	**Средняя**	**Высокая**
Низкая	Неактуальная	Неактуальная	Актуальная
Средняя	Неактуальная	Актуальная	Актуальная
Высокая	Актуальная	Актуальная	Актуальная
Очень высокая	Актуальная	Актуальная	Актуальная

10 УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

10.1. Угрозы утечки акустической (речевой) информации

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, при обработке ПДн в ИСПДн, возможно при наличии функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.

В ИСПДн «Сотрудники» Оператора функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами отсутствуют.

Вероятность реализации угрозы – маловероятно

Возможность реализации угрозы – 0,25 (низкая)

Опасность угрозы – низкая

Актуальность угрозы – неактуальная

10.2. Угрозы утечки видовой информации

Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптико-электронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео - и буквенно-цифровой информации, входящих в состав ИСПДн.

Помещения Оператора оборудованы системой охранной сигнализации (ОС). АРМ расположены так, что практически исключен визуальный доступ к монитору, на окнах имеются жалюзи или шторы.

Вероятность реализации угрозы – маловероятно

Возможность реализации угрозы – 0,25 (низкая)

Опасность угрозы – средняя

Актуальность угрозы – неактуальная

10.3. Угрозы утечки информации по каналам ПЭМИН

Угрозы утечки информации по каналу ПЭМИН, возможны из-за наличия паразитных электромагнитных излучений у элементов ИС.

Угрозы данного класса маловероятны для всех видов ИС, так как объективные предпосылки для осуществления угроз отсутствуют (малая численность единовременно обрабатываемых субъектов персональных данных, невысокая категория обрабатываемых персональных данных, сложность реализации угрозы – необходимость использования дорогостоящего оборудования квалифицированным специалистом, физические лица и криминальные группировки в качестве источника реализации угрозы предпочтут реализовать менее технически сложные угрозы безопасности).

Вероятность реализации угрозы – маловероятно

Возможность реализации угрозы – 0,25 (низкая)

Опасность угрозы – низкая

Актуальность угрозы – неактуальная

10.4. Утрата носителей информации

Угроза осуществляется пользователями ИС, вследствие человеческого фактора.

Оператором используются внешние носители информации, содержащей персональные данные, существуют журналы учета машинных носителей персональных данных, а также правила работы с машинными носителями персональных данных.

Вероятность реализации угрозы – маловероятно

Возможность реализации угрозы – 0,25 (низкая)

Опасность угрозы – низкая

Актуальность угрозы – неактуальная

10.5. Утрата и компрометация ключей и атрибутов доступа

Угроза осуществляется за счет действия человеческого фактора пользователей ИС, которые нарушают положения парольной политики в части их создания (создают простые или пустые пароли, не меняют пароли по истечении срока их жизни или компрометации и т.п.) и хранения (записывают пароли на бумажные носители, передают ключи доступа третьим лицам и т.п.) или не осведомлены о них.

У Оператора введена инструкция по организации парольной защиты, пользователи ознакомлены с ответственностью за не выполнение данной инструкции.

Вероятность реализации угрозы – маловероятно

Возможность реализации угрозы – 0,25 (низкая)

Опасность угрозы – низкая

Актуальность угрозы – неактуальная

10.6. Доступ к информации, ее модификация и уничтожение лицами, не имеющими прав доступа

Угроза осуществляется внешними нарушителями там, где расположены элементы ИС и средства защиты, а также происходит работа пользователей.

В здании, где расположена ИСПДн «Сотрудники» помещения закрываются на замки. Помещения Оператора оборудованы системой охранной сигнализации (ОС). В ИСПДн «Сотрудники» отсутствуют средства защиты информации от несанкционированного доступа, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации.

Вероятность реализации угрозы – средняя

Возможность реализации угрозы – 0,5 (средняя)

Опасность угрозы – средняя

Актуальность угрозы – актуальная

10.7. Утечка информации через порты ввода/вывода

Угроза осуществляется внутренними нарушителями категорий I и IV (пользователи и разработчики ИС).

Угроза реализуется путем подключения съемных носителей к компьютеру и несанкционированного копирования на них информации.

В соответствии с моделью нарушителя данная угроза является неактуальной.

Вероятность реализации угрозы – маловероятно
Возможность реализации угрозы – 0,25 (низкая)
Опасность угрозы – низкая
Актуальность угрозы – неактуальная

10.8. Воздействие вредоносных программ (вирусов)

Программно-математическое воздействие - это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой (вирусом) называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

1) скрывать признаки своего присутствия в программной среде компьютера;

2) обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;

3) разрушать (искажать произвольным образом) код программ в оперативной памяти;

4) выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирования, уничтожения, блокирования и т.п.);

5) сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);

6) искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

На всех элементах ИСПДн «Сотрудники» отсутствуют антивирусные средства, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, пользователи проинструктированы о мерах предотвращения вирусного заражения.

Вероятность реализации угрозы – средняя
Возможность реализации угрозы – 0,5 (средняя)
Опасность угрозы – средняя
Актуальность угрозы – актуальная

10.9. Установка ПО, не связанного с исполнением служебных обязанностей

Угроза осуществляется путем несанкционированной установки ПО внутренними нарушителями категорий I и IV (пользователи и разработчики ИС).

В соответствии с моделью нарушителя данная угроза является неактуальной.

Вероятность реализации угрозы – маловероятно
Возможность реализации угрозы – 0,25 (низкая)
Опасность угрозы – низкая
Актуальность угрозы – неактуальная

10.10. Внедрение или сокрытие недекларированных возможностей системного ПО и ПО для обработки персональных данных

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИСПДн считаются маловероятными ввиду использования лицензионного системного и программного обеспечения, разработчик которого, согласно модели нарушителя, не может являться нарушителем.

Вероятность реализации угрозы – маловероятно

Возможность реализации угрозы – 0,25 (низкая)

Опасность угрозы – низкая

Актуальность угрозы – неактуальная

10.11. Создание учетных записей теневых пользователей и неучтенных точек доступа в систему

Угроза осуществляется внутренними нарушителями категорий I и IV (пользователи и разработчики ИС). Угроза реализуется путем несанкционированного создания неучтенных точек доступа в систему (например, несанкционированное подключение нового компьютера к локальной сети), а также создание нерабочих учетных записей (тестовых, временных и т.д.).

В соответствии с моделью нарушителя данная угроза является неактуальной.

Вероятность реализации угрозы – маловероятно

Возможность реализации угрозы – 0,25 (низкая)

Опасность угрозы – низкая

Актуальность угрозы – неактуальная

10.12. Угроза «Анализ сетевого трафика» с перехватом информации за пределами контролируемой зоны

Эта угроза реализуется с помощью специальной программы-анализатора пакетов (sniffer), перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль. В ходе реализации угрозы нарушитель:

1) изучает логику работы ИСПДн - то есть, стремится получить однозначное соответствие событий, происходящих в системе, и команд, пересылаемых при этом хостами, в момент появления данных событий. В дальнейшем это позволяет злоумышленнику на основе задания соответствующих команд получить, например, привилегированные права на действия в системе или расширить свои полномочия в ней;

2) перехватывает поток передаваемых данных, которыми обмениваются компоненты сетевой операционной системы, для извлечения конфиденциальной или идентификационной информации (например, статических паролей пользователей для доступа к удаленным хостам по протоколам FTP и TELNET, не предусматривающих шифрование), ее подмены, модификации и т.п.

Оператором не осуществляется передача информации по сети Интернет.

Вероятность реализации угрозы – маловероятно

Возможность реализации угрозы – 0,25 (низкая)

Опасность угрозы – средняя

Актуальность угрозы – неактуальная

10.13. Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.

Сущность процесса реализации угрозы заключается в передаче запросов сетевым службам хостов ИС и анализе ответов от них. Цель - выявление используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей.

В ИСПДн «Сотрудники» отсутствуют средства межсетевого экранирования, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации.

Вероятность реализации угрозы – средняя

Возможность реализации угрозы – 0,5 (средняя)

Опасность угрозы – средняя

Актуальность угрозы – актуальная

10.14. Угроза выявления паролей по сети

Цель реализации угрозы состоит в получении НСД путем преодоления парольной защиты. Злоумышленник может реализовывать угрозу с помощью целого ряда методов, таких как простой перебор, перебор с использованием специальных словарей, установка вредоносной программы для перехвата пароля, подмена доверенного объекта сети (IP-spoofing) и перехват пакетов (sniffing). В основном для реализации угрозы используются специальные программы, которые пытаются получить доступ хосту путем последовательного подбора паролей. В случае успеха, злоумышленник может создать для себя «проход» для будущего доступа, который будет действовать, даже если на хосте изменить пароль доступа.

В ИСПДн «Сотрудники» отсутствуют средства антивирусной защиты и средства межсетевого экранирования, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации.

Вероятность реализации угрозы – средняя

Возможность реализации угрозы – 0,5 (средняя)

Опасность угрозы – средняя

Актуальность угрозы – актуальная

10.15. Угрозы типа «Отказ в обслуживании»

Эти угрозы основаны на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, когда операционная система оказывается не в состоянии обрабатывать поступающие пакеты.

Могут быть выделены несколько разновидностей таких угроз:

1) скрытый отказ в обслуживании, вызванный привлечением части ресурсов ИС-ПДн на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований к времени обработки запросов. Примерами реализации угроз подобного рода могут служить: направленный шторм эхо-запросов по протоколу ICMP (Ping flooding), шторм запросов на установление TCP-соединений (SYN-flooding), шторм запросов к FTP-серверу;

2) явный отказ в обслуживании, вызванный исчерпанием ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание), при котором легальные запросы не могут быть переданы через сеть из-за недоступности среды передачи, либо получают отказ в обслуживании ввиду переполнения очередей запросов, дискового пространства памяти и т.д. Примерами угроз данного типа могут служить шторм широковещательных ICMP-эхо-запросов (Smurf), направленный шторм (SYN-flooding), шторм сообщений почтовому серверу (Spam);

3) явный отказ в обслуживании, вызванный нарушением логической связности между техническим средствами ИСПДн при передаче нарушителем управляющих сооб-щений от имени сетевых устройств, приводящих к изменению маршрутно-адресных дан-ных (например, ICMP Redirect Host, DNS-flooding) или идентификационной и аутентификационной информации;

4) явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа «Land», «TearDrop», «Bonk», «Nuke», «UDP-bomb») или имеющих длину, превышающую максимально допустимый размер (угроза типа «Ping Death»), что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

Результатом реализации данной угрозы может стать нарушение работоспособности соответствующей службы предоставления удаленного доступа к ПДн в ИС, передача с одного адреса такого количества запросов на подключение к техническому средству в составе ИС, которое максимально может «вместить» трафик (направленный «шторм запросов»), что влечет за собой переполнение очереди запросов и отказ одной из сетевых служб или полная остановка ИС из-за невозможности системы заниматься ничем другим, кроме обработки запросов.

В ИСПДн «Сотрудники» отсутствуют средства межсетевого экранирования, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации.

Вероятность реализации угрозы – средняя

Возможность реализации угрозы – 0,5 (средняя)

Опасность угрозы – средняя

Актуальность угрозы – актуальная

10.16. Угрозы внедрения по сети вредоносных программ

К вредоносным программам, внедряемым по сети, относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. «Полноценные» сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, «подтолкнуть» пользователя к запуску зараженного файла.

Вредоносными программами, обеспечивающими осуществление НСД, могут быть:

1) программы подбора и вскрытия паролей;

2) программы, реализующие угрозы;

3) программы, демонстрирующие использование недекларированных возможностей программного и программно-аппаратного обеспечения ИСПДн;

4) программы-генераторы компьютерных вирусов;

5) программы, демонстрирующие уязвимости средств защиты информации и др.

В ИСПДн «Сотрудники» отсутствуют антивирусные средства антивирусной защиты и средства межсетевого экранирования, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации.

Вероятность реализации угрозы – средняя

Возможность реализации угрозы – 0,5 (средняя)

Опасность угрозы – средняя

Актуальность угрозы – актуальная

10.17. Утечка информации, передаваемой с использованием протоколов беспроводного доступа

Угроза реализуется путем перехвата информации, передаваемой по беспроводным сетям.

Оператором не используются протоколы беспроводного доступа.

Вероятность реализации угрозы – маловероятно

Возможность реализации угрозы – 0,25 (низкая)

Опасность угрозы – низкая

Актуальность угрозы – неактуальная

10.18. Перехват, модификация закрытого ключа ЭП

Угроза реализуется путем получения доступа к закрытому ключу ЭП либо путем перехвата закрытого ключа ЭП.

В ИСПДн «Сотрудники» не используется ЭП.

Вероятность реализации угрозы – маловероятно

Возможность реализации угрозы – 0,25 (низкая)

Опасность угрозы – низкая

Актуальность угрозы – неактуальная

10.19. Угрозы удаленного запуска приложений

Угроза заключается в стремлении запустить на хосте ИС различные предварительно внедренные вредоносные программы: программы-закладки, вирусы, «сетевые шпионы», основная цель которых - нарушение конфиденциальности, целостности, доступности информации и полный контроль за работой хоста. Кроме того, возможен несанкционированный запуск прикладных программ пользователей для несанкционированного получения необходимых нарушителю данных, для запуска управляемых прикладной программой процессов и др.

Выделяют три подкласса данных угроз:

1) распространение файлов, содержащих несанкционированный исполняемый код;

2) удаленный запуск приложения путем переполнения буфера приложений-серверов;

3) удаленный запуск приложения путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками, либо используемыми штатными средствами.

Типовые угрозы первого из указанных подклассов основываются на активизации распространяемых файлов при случайном обращении к ним. Примерами таких файлов могут служить: файлы, содержащие исполняемый код в вид документы, содержащие исполняемый код в виде элементов ActiveX, Java-апплетов, интерпретируемых скриптов (например, тексты на JavaScript); файлы, содержащие исполняемые коды программ. Для распространения файлов могут использоваться службы электронной почты, передачи файлов, сетевой файловой системы.

При угрозах второго подкласса используются недостатки программ, реализующих сетевые сервисы (в частности, отсутствие контроля за переполнением буфера). Настройкой системных регистров иногда удается переключить процессор после прерывания, вызванного переполнением буфера, на исполнение кода, содержащегося за границей буфера. Примером реализации такой угрозы может служить внедрение широко известного «вируса Морриса».

При угрозах третьего подкласса нарушитель использует возможности удаленного управления системой, предоставляемые скрытыми компонентами (например, «троянскими» программами типа Back. Orifice, Net Bus), либо штатными средствами управления и администрирования компьютерных сетей (Landesk Management Suite, Managewise, Back Orifice и т. п.). В результате их использования удается добиться удаленного контроля над станцией в сети.

В составе ИСПДн «Сотрудники» отсутствуют средства антивирусной защиты и средства межсетевого экранирования, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации.

Вероятность реализации угрозы – средняя

Возможность реализации угрозы – 0,5 (средняя)

Опасность угрозы – средняя

Актуальность угрозы – актуальная

10.20. Разглашение информации

Угроза осуществляется внутренними нарушителями категорий I и III (пользователи и администраторы ИС).

Угроза реализуется путем несанкционированной передачи информации третьим лицам.

В соответствии с моделью нарушителя данная угроза является неактуальной.

Вероятность реализации угрозы – маловероятно

Возможность реализации угрозы – 0,25 (низкая)

Опасность угрозы – средняя

Актуальность угрозы – неактуальная

10.21. Сокрытие ошибок и неправомерных действий пользователей и администраторов

Угроза реализуется внутренними нарушителями категорий I и III (пользователи и администраторы ИС).

В соответствии с моделью нарушителя данная угроза является неактуальной.

Вероятность реализации угрозы – маловероятно

Возможность реализации угрозы – 0,25 (низкая)

Опасность угрозы – низкая

Актуальность угрозы – неактуальная

10.22. Угроза появления новых уязвимостей вследствие невыполнения ответственными лицами своих должностных обязанностей

Угроза реализуется внутренними нарушителями категории III (администраторы ИС).

Угроза реализуется вследствие халатного отношения ответственного лица к своим должностным обязанностям.

В соответствии с моделью нарушителя данная угроза является неактуальной.

Вероятность реализации угрозы – маловероятно

Возможность реализации угрозы – 0,25 (низкая)

Опасность угрозы – средняя

Актуальность угрозы – неактуальная

10.23. Непреднамеренная модификация (уничтожение) информации

Угроза реализуется внутренними нарушителями категорий I и III (пользователи и администраторы ИС).

Угроза реализуется путем непреднамеренного воздействия на элементы ИС или содержащуюся в ней информацию.

В соответствии с моделью нарушителя данная угроза является неактуальной.

Вероятность реализации угрозы – маловероятно

Возможность реализации угрозы – 0,25 (низкая)

Опасность угрозы – низкая

Актуальность угрозы – неактуальная

10.24. Непреднамеренное отключение средств защиты

Угроза реализуется внутренними нарушителями категорий I и III (пользователи и администраторы ИС). Угроза реализуется путем случайного отключения средств защиты (антивирусного ПО, межсетевых экранов и т.д.).

Вероятность реализации угрозы повышается при отсутствии контроля доступа в контролируемую зону и к настройкам режимов средств защиты, а также неосведомленности пользователей о работе с ИСПДн «Сотрудники».

В соответствии с моделью нарушителя данная угроза является неактуальной.

Вероятность реализации угрозы – маловероятно

Возможность реализации угрозы – 0,25 (низкая)

Опасность угрозы – средняя

Актуальность угрозы – неактуальная

10.25. Стихийное бедствие

Угроза осуществляется вследствие возникновения различного рода природных катаклизмов (землетрясение, затопление и прочее).

Вероятность реализации угрозы – маловероятно

Возможность реализации угрозы – 0,25 (низкая)
Опасность угрозы – низкая
Актуальность угрозы – неактуальная

10.26. Выход из строя аппаратно-программных средств

Угроза реализуется вследствие окончания срока эксплуатации аппаратно-программных средств, нерегулярных проверок данных средств и перебоев в электропитании.

Оператором производится своевременная замена устаревших аппаратно-программных средств, проводятся регулярные проверки аппаратно-программных средств.

Вероятность реализации угрозы – маловероятно
Возможность реализации угрозы – 0,25 (низкая)
Опасность угрозы – низкая
Актуальность угрозы – неактуальная

10.27. Аварии (пожар, потоп, случайное отключение электричества)

Угроза осуществляется вследствие возникновения различного рода аварий в пределах контролируемой зоны.

Оператором производится своевременная замена устаревшего оборудования, коммуникаций и т.д., проводятся их регулярные проверки, установлена система охранной сигнализации.

Вероятность реализации угрозы – маловероятно
Возможность реализации угрозы – 0,25 (низкая)
Опасность угрозы – низкая
Актуальность угрозы – неактуальная

10.28. Действия криминальных групп и отдельных преступных элементов

Угроза осуществляется вследствие диверсии в отношении объектов ИС.

Двери помещений ИСПДн «Сотрудники» закрываются на замки. Помещения Оператора оборудованы системой охранной сигнализации и системой пожарной сигнализации.

Вероятность реализации угрозы – маловероятно
Возможность реализации угрозы – 0,25 (низкая)
Опасность угрозы – низкая
Актуальность угрозы – неактуальная

11 ВЫВОДЫ

На данном этапе функционирования ИСПДн «Сотрудники» выявлены следующие актуальные угрозы из списка угроз безопасности под номерами:

10.6. Доступ к информации, ее модификация и уничтожение лицами, не имеющими прав доступа

10.8. Воздействие вредоносных программ (вирусов)

10.13. Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.

10.14. Угроза выявления паролей по сети

10.15. Угрозы типа «Отказ в обслуживании»

10.16. Угрозы внедрения по сети вредоносных программ

10.19. Угрозы удаленного запуска приложений

ПРИЛОЖЕНИЕ Л

УТВЕРЖДАЮ

Генеральный директор ООО «Трехгорный керамический завод»

_____ В.Ю. Горбатов

«____» _____ 2018 г.

Описание технологического процесса обработки информации
информационной системы обработки персональных данных
«Сотрудники»

2018 г.

1. Владелец объекта информатизации

ООО «Трехгорный керамический завод (далее – Оператор).

2. Назначение объекта информатизации

Информационная система персональных данных «Сотрудники» ООО «Трехгорный керамический завод» (далее – ИСПДн) предназначена для обработки информации ограниченного доступа, в том числе ПДн, в целях, возникающих в процессе реализации трудовых отношений между работником и Оператором.

3. Организация охраны и контроля доступа

Кабинеты, в которых размещены компоненты ИСПДн (далее – защищаемые помещения), расположены на территории Оператора. Руководителем Оператора утвержден документ, регламентирующий доступ к компонентам ИСПДн, внутриобъектовый и пропускной режимы и распространяющий своё действие на всей территории Оператора. Оператором принимаются все необходимые организационно-технические меры, исключающие бесконтрольный доступ в защищаемые помещения лиц, не допущенных к работе с ИСПДн. Защищаемые помещения оборудованы прочными, надёжно-запирающимися дверями. Кабинеты оборудованы пожарной сигнализацией.

4. Состав ИСПДн

Объекты доступа:

- средство вычислительной техники в целом;
- периферийное оборудование;
- машинные носители информации, в том числе съёмные: накопители на жестких магнитных дисках (НЖМД), флэш-накопители;
- коммуникационные порты системного блока: RJ45, USB-порты;
- приводы оптических дисков, дистрибутивы системного и прикладного программного обеспечения, средств защиты информации;
- каталоги (файлы) системного и прикладного программного обеспечения, средств защиты информации, в том числе файлы настроек;
- каталоги (файлы) пользователей операционных систем и базы данных прикладного программного обеспечения, содержащие информацию ограниченного доступа, в том числе персональные данные;

- базы данных сторонних информационных систем, содержащие персональные данные, с которыми осуществляется взаимодействие.

Субъекты доступа:
- администратор безопасности ИСПДн;
- пользователи ИСПДн;
- обслуживающий персонал (осуществляет техническое обслуживание средств вычислительной техники, программного обеспечения).

Средства доступа к информации в ИСПДн:
– штатные средства операционных систем;
- прикладное программное обеспечение.

Источники данных в ИСПДн:
– работники Оператора;

ИСПДн состоит из комплекса СВТ, объединённых в единую информационную систему средствами связи без использования технологии удалённого доступа.

Полный перечень компонентов ИСПДн представлен в Техническом паспорте ИСПДн.

5. Обеспечение безопасности ИСПДн

Приказом руководителя Оператора назначены ответственный за обеспечение безопасности ПДн и администратор безопасности ИСПДн.

Разработан и утверждён комплект организационно-распорядительной документации, регламентирующей организацию обработки и обеспечение безопасности ПДн, обрабатываемых на объектах Оператора, в том числе в ИСПДн (далее – ОРД). Разработана и утверждена Модель угроз безопасности ПДн при их обработке в ИСПДн, содержащая актуальный перечень угроз безопасности ПДн при их обработке в ИСПДн. Осуществляется периодический контроль актуальности данных документов.

Работники Оператора, допущенные к работе с ИСПДн, ознакомлены с положениями законодательства Российской Федерации в сфере организации обработки и обеспечения безопасности ПДн и ОРД и выполняют в полной мере возложенные на них функции в соответствии с присвоенной им в ИСПДн ролью.

Любые действия связанные с используемыми в ИСПДн СЗИ (настройка, обновление и т.п.) выполняет администратор безопасности ИСПДн в соответствии с

технической и эксплуатационной документацией на данные СЗИ.

Организованы и соблюдаются антивирусная и парольная защиты в соответствии со специально-разработанными инструкциями.

6. Доступ к информационным ресурсам

6.1 Общая часть

Доступ к ИСПДн имеют только работники Оператора на основании приказов или иных утверждённых руководителем Оператора документов.

Права доступа работников Оператора к информационным ресурсам и компонентам ИСПДн ограничены в соответствии с исполняемыми ими служебными (трудовыми) обязанностями и функциями в ИСПДн и зафиксированы в соответствующей локальной нормативной документации Оператора.

6.2 Начало сеанса работы

После включения СВТ происходит загрузка операционной системы и появляется окно ввода учётных данных пользователя ИСПДн. После ввода корректных учётных данных происходит окончательная загрузка профиля пользователя. Если его персональный идентификатор (логин) не зарегистрирован в системе защиты информации от НСД Dallas Lock 8.0-K (далее – СЗИ от НСД) или он ввёл некорректную аутентификационную информацию (пароль), то доступ к информационным ресурсам для него будет недоступен до ввода корректных данных.

Логин и пароль каждого работника Оператора, допущенного к работе с ИСПДн, являются уникальными. Все используемые в ИСПДн пароли соответствуют требованиям специально-разработанной инструкции. Плановая и внеплановая смена паролей производится в соответствии с данной инструкцией.

6.3 Регистрация и удаление пользователей ИСПДн, назначение прав доступа

Добавление новых пользователей в ИСПДн или блокирование доступа старым (путём удалениях их учётных записей) осуществляется администратором безопасности ИСПДн средствами системы защиты информации от НСД.

При удалении учётных записей пользователей ИСПДн администратором безопасности ИСПДн производится удаление ассоциированных с ними каталогов, если хранимая в них информация более не требуется для исполнения другими работниками Оператора своих служебных (трудовых) обязанностей.

Разграничение прав доступа пользователей ИСПДн к информационным ресурсам ИСПДн осуществляется администратором безопасности ИСПДн средствами СЗИ от НСД на основании соответствующего документа.

6.4 Обработка персональных данных в ИСПДн

Документы, содержащие ПДн, предоставляются работниками. Сотрудники Оператора вводят ПДн в ИСПДн вручную, посредством заполнения полей форм созданных с помощью пакета офисных программ.

Формы документов, созданные с помощью пакета офисных программ, хранятся непосредственно на СВТ пользователей в разрешённых администратором безопасности ИСПДн каталогах.

Осуществляется передача ПДн в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, в аутсорсинговую компанию IS-consult на материальных носителях информации.

Обновление неактуальных персональных данных, обрабатываемых в ИСПДн, осуществляется имеющими на то соответствующие полномочия пользователями ИСПДн путём внесения изменений в информацию, содержащуюся в полях форм, созданных с помощью пакета офисных программ.

6.5 Уничтожение персональных данных

Уничтожение ПДн осуществляется имеющими на то соответствующие полномочия работниками Оператора в случае утраты Оператором правовых оснований обработки.

Уничтожение бумажных и машинных носителей ПДн производится способами, исключающими возможность дальнейшей обработки зафиксированных на них ПДн.

Уничтожение файлов и каталогов, содержащих ПДн, остаточной информации осуществляется с помощью подсистемы гарантированного уничтожения остаточной информации, входящей в состав СЗИ от НСД. Запрещается удалять информацию иными способами.

6.6 Завершение сеанса работы

По окончании работы пользователь ИСПДн выполняет штатную процедуру завершения работы операционной системы, выключает СВТ и помещает бумажные и машинные носители ПДн, в запирающиеся металлические шкафы.

ПРИЛОЖЕНИЕ М

ООО «Трехгорный керамический завод»

УТВЕРЖДАЮ

Ген. Директор
ООО «Трехгорный керамический завод

_____В.Ю. Горбатов
___ _____ _____г.

АКТ

от ___ _____ №_____
_____г.

определения уровня защищенности персональных данных информационной системы персональных данных «Сотрудники»

Составлен комиссией:

Председатель:

	Ген. директор	Горбатов В.Ю.

Члены комиссии:

1.	Начальник отдела кадров	Лапина А.С.
2.	Сотрудник отдела кадров	Афанасьева Г.Н.
3.	Начальник технического отдела	Федорчук Е.О.

Комиссия установила, что согласно постановлению Правительства от 01.11.12 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»:

— ИСПДн является информационной системой, обрабатывающей иные категории персональных данных <100000 субъектов персональных данных, являющихся сотрудниками оператора.

— для ИСПДн «Сотрудники» актуальными являются угрозы 3 типа.

На основании анализа исходных данных комиссия решила, что для персональных данных ИСПДн «Сотрудники» необходимо обеспечить 4 уровень защищенности.

Председатель:		
Ген. директор	_____	Горбатов В.Ю.
Члены комиссии:		
Начальник отдела кадров	_____	Лапина А.С.
Сотрудник отдела кадров	_____	Афанасьева Г.Н.
Начальник технического отдела	_____	Федорчук Е.О.

Продолжение приложения М

ООО «Трехгорный керамический завод»

ПРИКАЗ

от ___ _____ _____г. №_____

О назначении ответственного за обеспечение безопасности информации

С целью организации работ по обеспечению безопасности персональных данных при их обработке в ООО «Трехгорный керамический завод» в соответствии с требованиями Федерального Закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ, постановления Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 №1119.

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемую Инструкцию ответственного за обеспечение безопасности информации.
2. Назначить ответственным за обеспечение безопасности информации ООО «Трехгорный керамический завод» Федорчука Евгения Олеговича.
3. Возложить на Федорчука Евгения Олеговича обязанности в соответствии с Инструкцией ответственного за обеспечение безопасности информации.
4. Контроль за выполнением требований настоящего приказа оставляю за собой.

Ген. директор
ООО «Трехгорный керамический завод» _____ В.Ю. Горбатов

С приказом ознакомлен:
Начальник технического отдела _____ Е.О. Федорчук

_____ г.

ООО «Трехгорный керамический завод»

ПРИКАЗ

от ___ _____ _____г. №_____

О назначении ответственного за организацию обработки персональных данных

С целью организации работ по обеспечению безопасности персональных данных при их обработке в ООО «Трехгорный керамический завод» в соответствии с требованиями Федерального Закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ.

ПРИКАЗЫВАЮ:

5. Утвердить и ввести в действие Инструкцию ответственного за организацию обработки персональных данных.

6. Назначить ответственным за организацию обработки персональных данных в ООО «Трехгорный керамический завод» Афанасьеву Галину Васильевну.

7. Возложить на Афанасьеву Галину Васильевну обязанности в соответствии с Инструкцией ответственного за организацию обработки персональных данных.

8. Контроль за выполнением требований настоящего приказа оставляю за собой.

Ген. директор
ООО «Трехгорный керамический завод» _____ В.Ю. Горбатов

С приказом ознакомлен:
Начальник отдела кадров _____ Г.В. Афанасьева

_____ г.

ПРИЛОЖЕНИЕ Н

УТВЕРЖДАЮ

Генеральный директор ООО «Трехгорный керамический завод»

_____ В.Ю. Горбатов

«____» _____ 2018 г.

Политика обработки персональных данных
информационной системы обработки персональных данных
«Сотрудники»

2018г.

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. В целях гарантирования выполнения норм федерального законодательства в полном объеме ООО «Трехгорный керамический завод» (далее – Оператор) считает своими задачами соблюдение принципов законности, справедливости и конфиденциальности при обработке персональных данных, а также обеспечение безопасности процессов их обработки.

1.2. Настоящая политика в области обработки и защиты персональных данных в ООО «Трехгорный керамический завод» (далее – политика) характеризуется следующими признаками:

1.2.1. Разработана в целях обеспечения реализации требований законодательства РФ в области обработки персональных данных субъектов персональных данных (физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных).

1.2.2. Раскрывает основные категории персональных данных, обрабатываемых оператором, цели, способы и принципы обработки оператором персональных данных, права и обязанности оператора при обработке персональных данных, права субъектов персональных данных, а также включает перечень мер, применяемых оператором в целях обеспечения безопасности персональных данных при их обработке.

1.2.3. Является общедоступным документом, декларирующим концептуальные основы деятельности оператора при обработке персональных данных.

III. ИНФОРМАЦИЯ ОБ ОПЕРАТОРЕ

3.1. Наименование: ООО «Трехгорный керамический завод»

3.2. ИНН: 7405008850

3.3. Фактический адрес: 456082, г. Трехгорный Челябинской области, ул. Заречная,1А, а/я 254.

3.4. Тел., факс: (351-91) 5-70-33

IV. ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Политика Оператора в области обработки персональных данных определяется в соответствии со следующими нормативными правовыми актами:

4.1.1. Конституцией Российской Федерации.

4.1.2. Трудовым кодексом Российской Федерации.

4.1.3. Гражданским кодексом Российской Федерации.

4.1.4. Федеральным законом от 19.12.2005 №160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».

4.1.5. Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных».

4.1.6. Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».

4.2. Во исполнение настоящей Политики руководящим органом Оператора утверждены следующие локальные нормативные правовые акты:

4.2.1. Положение об обработке персональных данных с использованием средств автоматизации.

4.2.2. Положение о порядке обработки персональных данных без использования средств автоматизации.

4.2.3. Регламент резервного копирования и восстановления данных.

4.2.4. Инструкция о порядке работы с персональными данными.

4.2.5. Акт определения уровня защищенности информационной системы персональных данных.

4.2.6. Инструкция ответственного за обеспечение безопасности информации.

4.2.7. Инструкция ответственного за организацию обработки персональных данных.

4.2.8. Инструкция пользователя информационной системы.

4.2.9. Типовая форма согласия субъектов на обработку персональных данных и др.

V. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Оператор обрабатывает персональные данные исключительно в следующих целях:

5.1.1. Исполнения положений нормативных актов.

5.1.2. Принятия решения о трудоустройстве кандидата у Оператора.

5.1.3. Заключения и выполнения обязательств по трудовым договорам, договорам гражданско-правового характера и договорам с контрагентами.

VI. КАТЕГОРИИ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. В информационных системах персональных данных оператора обрабатываются следующие категории персональных данных:

6.1.1. Персональные данные сотрудников.

6.1.2. Персональные данные соискателей.

6.1.3. Персональные данные кандидатов на замещение вакантных должностей.

VII. ОСНОВНЫЕ ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Оператор в своей деятельности обеспечивает соблюдение принципов обработки персональных данных, указанных в ст.5 Федерального закона 152-ФЗ «О персональных данных».

7.2. Оператор не осуществляет обработку биометрических персональных данных (сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных).

7.3. Оператор не выполняет обработку специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

7.4. Оператор не производит трансграничную (на территории иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу) передачу персональных данных.

7.5. Оператором созданы общедоступные источники персональных данных (справочники, адресные книги). Персональные данные, сообщаемые субъектом (фамилия, имя, отчество, год и место рождения, адрес и др.), включаются в такие источники только с письменного согласия субъекта персональных данных.

7.6. Оператором не используются для обработки персональных данных базы данных, находящиеся за пределами границ Российской Федерации.

VIII. СВЕДЕНИЯ О ТРЕТЬИХ ЛИЦАХ, УЧАВСТВУЮЩИХ В ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. В целях соблюдения законодательства РФ, для достижения целей обработки, а также в интересах и с согласия субъектов персональных данных Оператор в ходе своей деятельности предоставляет персональные данные следующим организациям:

8.1.1. Федеральной налоговой службе

8.1.2. Пенсионному фонду России

8.1.3. Лицензирующим и/или контролирующим органам государственной власти и местного самоуправления.

IX. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ

9.1. Оператор при обработке персональных данных принимает все необходимые правовые, организационные и технические меры для их защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении них. Обеспечение безопасности персональных данных достигается, в частности, следующими способами:

9.1.1. Назначением ответственных за организацию обработки персональных данных.

9.1.2. Осуществлением внутреннего контроля и/или аудита соответствия обработки персональных данных ФЗ от 27.07.2006 №152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, локальным актам.

9.1.3. Ознакомлением работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, в том числе с требованиями к защите персональных данных, локальными актами в отношении обработки персональных данных, и (или) обучением указанных сотрудников.

9.1.4. Определением угроз безопасности персональных данных при их обработке в информационных системах.

9.1.5. Применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах, необходимых для выполнения требований к защите персональных данных.

9.1.6. Оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы.

9.1.7. Учетом машинных носителей персональных данных.

9.1.8. Выявлением фактов несанкционированного доступа к персональным данным и принятием соответствующих мер.

9.1.9. Восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

9.1.10. Установлением правил доступа к персональным данным, обрабатываемым в информационной системе, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе.

9.1.11. Контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационной системы.

X. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. Субъект персональных данных имеет право на получение сведений об обработке его персональных данных Оператором.

10.2. Субъект персональных данных вправе требовать от Оператора, который их обрабатывает, уточнения этих персональных данных, их блокирования или уничтожения в случае, если они являются неполными, устаревшими, неточными, незаконно полученными или не могут быть признаны необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

10.3. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами.

10.4. Для реализации своих прав и защиты законных интересов субъект персональных данных имеет право обратиться к Оператору. Тот рассматривает любые обращения и жалобы со стороны субъектов персональных данных, тщательно расследует факты нарушений и принимает все необходимые меры для их немедленного устранения, наказания виновных лиц и урегулирования спорных и конфликтных ситуаций в досудебном порядке.

10.5. Субъект персональных данных вправе обжаловать действия или бездействие Оператора путем обращения в уполномоченный орган по защите прав субъектов персональных данных.

10.6. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и/или компенсацию морального вреда в судебном порядке.

XI. КОНТАКТНАЯ ИНФОРМАЦИЯ

11.1. Ответственным за организацию обработки и обеспечения безопасности персональных данных у Оператора назначен начальник технического отдела Федорчук Евгений Олегович.

11.2. Уполномоченным органом по защите прав субъектов персональных данных является федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), управление по защите прав субъектов персональных данных.

XII. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

12.1. Настоящая политика является внутренним документом Оператора, общедоступной и подлежит размещению на официальном сайте Оператора.

12.2. Настоящая политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных, но не реже одного раза в три года.

12.3. Контроль исполнения требований настоящей политики осуществляется ответственным за организацию обработки персональных данных Оператора.

12.4. Ответственность должностных лиц Оператора, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с законодательством Российской Федерации и внутренними документами Оператора.

ЛИСТ ОЗНАКОМЛЕНИЯ
с Политикой обработки и защиты персональных данных (для сотрудников)

Дата ознакомления	ФИО сотрудника	Должность сотрудника	Подпись сотрудника