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

РАБОТА ПРОВЕРЕНА
Рецензент, начальник технического
отдела, главный инженер
АО «Гранит Информ»
_____ А.С.Жаворонкин
_____ 2018 г.

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

Аттестация информационной системы персональных данных «Бухгалтерия» ООО «Завод углеродных и композиционных материалов»

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ – 10.05.03.2018.269.ПЗ ВКР

Консультанты

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

Руководитель проекта,
ген. директор ООО «Диджитер»
_____С.А. Сабельников
_____ 2018 г.

Автор проекта,
студент группы КЭ-530
_____ А.Ф. Морар
_____ 2018 г.

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

Челябинск 2018

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

Высшая школа электроники и компьютерных наук
Кафедра «Защита информации»

Специальность 10.05.03 «Информационная безопасность автоматизированных систем»

УТВЕРЖДАЮ
Заведующий кафедрой
_____ А.Н. Соколов

_____ 2018 г.

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

Морар Анастасии Федоровны

Группа *КЭ-530*

1. Тема работы

Аттестация ИСПДн «Бухгалтерия» Общества с ограниченной ответственностью «Завод углеродных и композиционных материалов»

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

2. Срок сдачи студентом законченной работы *30.05.2018*

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)

4.1 Этап обследования объекта информатизации

4.2 Разработка технической документации

4.3 Этап аттестационных испытаний объекта информатизации

4.4 Безопасность жизнедеятельности

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

Презентация «Аттестация информационной системы персональных данных «Бухгалтерия» ООО «Завод углеродных и композиционных материалов» в формате PowerPoint 2007 (pptx). Количество слайдов

Всего ___ листов

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

Раздел	Консультант	Подпись, дата	
		Задание выдал (консультант)	Задание принял (студент)
Экономическая часть	Сабельников С.А.		
Безопасность жизнедеятельности	Глотова Н.В.		

7. Дата выдачи задания *25 января 2018*

Руководитель,
Ст. преп._____ С.А. Сабельников

Задание принял к исполнению _____ А.Ф. Морар

КАЛЕНДАРНЫЙ ПЛАН

Наименование этапов выпускной квалификационной работы (проекта)	**Срок выполнения этапов работы**	**Отметки о выполнении руководителя**
Введение		
1 Этап обследования объекта информатизации		
2 Разработка технической документации		
3 Этап аттестационных испытаний объекта информатизации		
4 Безопасность жизнедеятельности		
Заключение		
Библиографический список		
Предзащита ВКР		
Защита ВКР		

Заведующий кафедрой _____ А.Н. Соколов

Руководитель работы _____ С.А.Сабельников

Студент _____ А.Ф.Морар

АННОТАЦИЯ

Морар А.Ф. Аттестация ИСПДн «Бухгалтерия» Общества с ограниченной ответственностью «Завод углеродных и композиционных материалов» – Челябинск: ЮУрГУ, КЭ-530, 148с., 2 ил., 12 табл., библиогр. список – 15 наим., 14 прил.

Выпускная квалификационная работа выполнена с целью проведения аттестации информационной системы персональных данных «Бухгалтерия» Общества с ограниченной ответственностью «Завод углеродных и композиционных материалов».

В выпускной квалификационной работе отражены все этапы проведения аттестации ИСПДн, от сбора исходных данных до заключения о соответствии нормативным документам РФ по защите персональных данных.

В процессе выполнения квалификационной работы было проведено обследование ИСПДн, созданы все необходимые документы, регламентирующие порядок защиты информации, а также описывающие информационную систему персональных данных предприятия. Были проведены аттестационные испытания на соответствие требованиям по защите информации от несанкционированного доступа.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

По законодательству Российской Федерации основным документом по обеспечению защиты персональных данных является федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных», согласно которому любая организация должна защищать информацию о своих сотрудниках и клиентах. В соответствии с требованиями законодательства необходимо разработать комплект организационно-распорядительной документации, соответствующий нормативно-правовым актам РФ в области обеспечения защиты персональных данных и периодически проводить оценку защищенности объектов информатизации по требованиям безопасности информации согласно приказу ФСТЭК России № 21 от 18.02.2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Таким образом, актуальность моей работы обоснована требованием законодательства.

Объектом выпускной квалификационной работы является Общество с ограниченной ответственностью «Завод углеродных и композиционных материалов».

Предметом выпускной квалификационной работы является информационная система персональных данных (ИСПДн) «Бухгалтерия» Общества с ограниченной ответственностью «Завод углеродных и композиционных материалов», аттестацию, которой проводил АО «Гранит Информ».

Целью данной дипломной работы является аттестация по требованиям безопасности информации ИСПДн «Бухгалтерия». Для реализации поставленной цели будем руководствоваться порядком проведения аттестации, утвержденным Положением по аттестации объектов информатизации по требованиям безопасности информации:

– анализ исходных данных по аттестуемому объекту информатизации;

– предварительное ознакомление с объектом информатизации;

– проведение экспертного обследования объекта информатизации и разработка документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации;

– проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств;

– проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации;

– анализ результатов экспертного обследования и комплексных аттестационных испытаний информатизации и утверждение заключения по результатам аттестации[1].

ГЛАВА 1. ОБСЛЕДОВАНИЕ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

1.1 Правовые основы проведения аттестации

Одной из угроз информационной безопасности Российской Федерации, указанных в Доктрине информационной безопасности [2], является рост масштабов компьютерной преступности, увеличение числа преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных в информационных системах. При этом методы, способы и средства таких преступлений становятся все изощрённее.

В соответствии с пунктом 4 части 2 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» обеспечение безопасности персональных данных достигается в частности оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных[3].

В соответствии с пунктом 6 Состава и содержания мер, утвержденных приказом ФСТЭК России от 18 февраля 2013 г. № 21[4], оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится оператором самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. При этом составом и содержанием мер, утвержденными приказом ФСТЭК России от 18 февраля 2013 г. № 21, форма оценки эффективности, а также форма и содержание документов, разрабатываемых по результатам оценки, не установлены.

Таким образом, решение по форме оценки эффективности мер по обеспечению безопасности персональных данных и документов, разрабатываемых по результатам оценки эффективности, принимается оператором самостоятельно или по соглашению с лицом, привлекаемым для проведения оценки эффективности реализованных мер по обеспечению безопасности ПДн.

Оценка эффективности реализованных мер может быть проведена в рамках работ по аттестации информационной системы персональных данных в соответствии с национальным стандартом ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения».

Аттестация – оценка соответствия требованиям безопасности информации, применяемые к ИСПДн как к защищаемым объектам информатизации. Оценка соответствия является обязательной процедурой, завершающей этап ввода в строй ИСПДн с внедренной в нее системой защиты.

Аттестация – комплекс организационно-технических мероприятий, в результате которых подтверждается, что объект информатизации соответствует требо-

ваниям стандартов или иных нормативных документов по безопасности информации[1].

Целью проведения аттестации является подтверждение работоспособности информационной системы организации с внедренными в ее инфраструктуру средствами и системами защиты персональных данных и подтверждение соответствия каждой идентифицированной ИСПДн требованиям к безопасности информации.

В соответствии с «Положением по аттестации объектов информатизации по требованиям безопасности», утвержденным председателем Гостехкомиссии при Президенте РФ 25.11.1994 г., система аттестации объектов информатизации является составной частью единой системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации[1].

Деятельность системы аттестации организует федеральный орган по сертификации продукции и аттестации объектов информатизации по требованиям безопасности информации, которым является ФСТЭК России.

Наличие на объекте информатизации действующего «Аттестата соответствия» дает право обработки информации с уровнем конфиденциальности и на период времени, установленными в «Аттестате соответствия».

Органы по аттестации аккредитуются ФСТЭК России. Правила аккредитации определяются «Положением об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации». Аккредитация проводится только при условии наличия у органа по аттестации лицензий на соответствующие виды деятельности.

Разработка данной дипломной работы, целью которой является проведение аттестации ИСПДн «Бухгалтерия» Общества с ограниченной ответственностью «Завод углеродных и композиционных материалов», реализована на базе предприятия-лицензиата в области обеспечения безопасности информации АО «Гранит Информ».

1.2 Анализ технического задания

Для получения «Аттестата соответствия» ООО «Завод углеродных и композиционных материалов» заблаговременно направило в орган по аттестации техническое задание на проведение аттестации объекта информатизации по требованиям безопасности информации, по форме, приведенной в приложении А.

Техническое задание представляет собой документ, отражающий цели проведения аттестации, объем работы, требования к сроку выполнения работ, перечень нормативно-правовых документов, на основе которых, должна проводиться аттестация, и обязанности заказчика и исполнителя работ.

Объектом информатизации ООО «Завод углеродных и композиционных материалов» является информационная система персональных данных, представляющая собой автоматизированное рабочее место.

Обработка персональных данных субъектов ИСПДн «Бухгалтерия» ООО «ЗУКМ» производится на основании ст. 6 ФЗ от 27 июля 2006 г. № 152-ФЗ «О персональных данных». ПДн используются для обработки, регистрации сведений, необходимых для ведения бухгалтерского учета.

На основании исходных данных орган по аттестации «Гранит Информ» выбрал схему аттестации и принял решение о проведении аттестации объекта информатизации ИСПДн «Бухгалтерия».

1.3 Разработка программы и методики аттестационных испытаний

По результатам рассмотрения технического задания и анализа исходных данных аттестуемого объекта органом по аттестации должна быть разработана программа аттестационных испытаний. Так как программы и методики аттестационных испытаний применительно для ИСПДн нет, она была разработана аттестационной комиссией на основе «Положения по аттестации объектов информатизации по требованиям безопасности информации»[1]. Программа и методика предусматривает перечень работ и их продолжительность, методики испытаний, определяются количественный и профессиональный состав аттестационной комиссии, назначаемый органом по аттестации объекта информатизации, необходимость использования контрольной аппаратуры и тестовых средств на аттестуемом объекте информатизации.

Программа и методика аттестационных испытаний представлена в приложении Б.

1.4 Обследование ИСПДн

На этапе обследования ИСПДн нами проводился опрос пользователей и администратора с целью определения специфики процесса обработки ПД в ИСПДн.

Материалы, полученные в ходе работ по обследованию ИСПДн, используются для дальнейших работ: анализ ИСПДн, разработки организационно-распорядительных документов.

В первую очередь проводится анализ таких документов, как приказ «Об организации работ по обеспечению безопасности персональных данных при их обработке в ИСПДн», перечень ПДн, приказ «Об определении границ контролируемой зоны объекта информатизации».

1.4.1 Приказ «Об организации работ по обеспечению безопасности персональных данных при их обработке в ИСПДн»

Для организации работ по обеспечению безопасности ПДн при их обработке в ИСПДн в соответствии с требованиями Постановления «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1 ноября 2012 г. № 1119 необходим организационный документ. В нем должны быть назначены ответственный за обеспечение безопасности ПДн в организации, администратор безопасности и сотрудники, доступ которых к ПДн необходим для выполнения служебных обязанностей. Ответственный осуществляет контроль соблюдения сотрудниками, обрабатывающими ПДн, правил обработки и обеспечения безопасности персональных данных. Администратор безопасности обеспечивает защищенность ПДн. А также в приказе создается комиссия для определения уровня защищенности ИСПДн.

1.4.2 Перечень ПДн, подлежащих защите в ИСПДн

В ИСПДн «Бухгалтерия» ООО «Завод углеродных и композиционных материалов» используются следующие ПДн:

– фамилия, имя, отчество;
– паспортные данные;
– адрес регистрации;
– фактический адрес проживания;
– дата рождения;
– ИНН;
– имущественное положение;
– сведения об образовании;
– свидетельство о рождении;
– СНИЛС;
– семейное положение;
– состав семьи.

1.4.3 Приказ «Об определении границ контролируемой зоны объекта информатизации»

Одним из основных организационных мероприятий по защите информации является установление контролируемой зоны вокруг ИСПДн.

Контролируемая зона – это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств. Все элементы ИСПДн должны располагаться в пределах контролируемой зоны[4].

Контролируемой зоной объекта информатизации – ИСПДн «Бухгалтерия» является охраняемая территория Общества с ограниченной ответственностью

«Завод углеродных и композиционных материалов» по адресу: г. Челябинск, Челябинский электродный завод. Граница контролируемой зоны определена приказом «Об определении границ контролируемой зоны» № 349 от 16.04.2018. Минимальное расстояние от ОТСС до КЗ составляет 15 метров.

1.4.4 Инструкции

В организационные меры по обеспечению безопасности ПДн при их обработке в ИСПДн необходимо наличие инструкций, поэтому на объекте информатизации в ходе выполнения ВКР был проведен анализ инструкций:

– инструкция администратору содержит следующие положения: обязанности администратора безопасности, права администратора безопасности, ответственность администратора безопасности, порядок резервного копирования и восстановления информационных ресурсов ИСПДн.

– инструкция пользователю содержит основные задачи и функции пользователей ИСПДн, обязанности пользователей ИСПДн, права пользователей ИСПДн и ответственность пользователей ИСПДн.

– инструкция по организации антивирусной защиты определяет требования к организации защиты ИСПДн «Бухгалтерия» ООО «Завод углеродных и композиционных материалов» от разрушающего воздействия компьютерных вирусов и иного вредоносного программного обеспечения и устанавливает ответственность руководителя и сотрудников, эксплуатирующих и сопровождающих ИСПДн, за их выполнение.

– инструкция по резервному копированию и восстановлению информационных ресурсов определяет правила и объемы резервирования, а также порядок восстановления работоспособности ИСПДн «Бухгалтерия» ООО «Завод углеродных и композиционных материалов».

– инструкция по организации парольной защиты в ИСПДн регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в ИСПДн «Бухгалтерия» ООО «Завод углеродных и композиционных материалов», а также контроль действий пользователей при работе с паролями.

– инструкция по разбирательству инцидентов информационной безопасности в ИСПДн устанавливает порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений, а так же выявления, разбирательства и предотвращения иных инцидентов

информационной безопасности в ИСПДн «Бухгалтерия» ООО «Завод углеродных и композиционных материалов».

– инструкция по обеспечению безопасности средств криптографической защиты информации (СКЗИ) устанавливает порядок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации.

1.4.5 Журналы учета

В ходе выполнения ВКР на объекте информатизации была проведена проверка на наличие журналов учета лиц, допущенных к работе с ПД, и машинных носителей в ИСПДн.

На данном этапе нами был составлен документ «Акт обследования ИСПДн», представленный в приложении В.

1.5 Определение уровня защищенности ИСПДн

В соответствии с Постановлением «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1 ноября 2012 г. № 1119, требования по защите ПДн в ИСПДн зависят от уровня защищенности ИСПДн.

Уровень защищенности – это комплексный показатель, который характеризует выполнение требований, нейтрализующих угрозы безопасности ИСПДн[6].

Требованиями к защите ПДн при их обработке в информационных системах (утв. Постановлением Правительства от 1 ноября 2012 г. № 1119) установлены 4 уровня защищенности ПДн, различающихся перечнем необходимых к выполнению требований по защите информационных систем.

Для определения уровня защищенности необходимо установить категорию обрабатываемых ПДн субъектов, вид обработки по форме отношений между субъектами и организацией, количество субъектов, а также тип угроз актуальных для информационной системы.

Категории обрабатываемых ПДн, подразделяются на 4 группы:

1 группа – специальные категории ПДн, к которым относятся информация о национальной и расовой принадлежности субъекта, о религиозных, философских либо политических убеждениях, информацию о здоровье и интимной жизни субъекта;

2 группа – биометрические ПДн, то есть данные, характеризующие биологические или физиологические особенности субъекта, например, фотография или отпечатки пальцев;

3 группа – общедоступные ПДн, то есть сведения о субъекте, полный и неограниченный доступ к которым предоставлен самим субъектом;

4 группа – иные категории ПДн, не представленные в трех предыдущих группах.

Данная аттестуемая ИСПДн «Бухгалтерия» относится к категории «Иные», так как в ней не обрабатываются специальные, биометрические и общедоступные категории ПДн.

По форме отношений между организацией и субъектами обработка подразделяется на 2 вида:

– обработка ПДн работников (субъектов, с которыми организация связана трудовыми отношениями);

– обработка ПДн субъектов, не являющихся работниками данной организации.

В данном случае ИСПДн «Бухгалтерия» ООО «Завод углеродных и композиционных материалов» обрабатывает ПДн субъектов, с которыми организация связана трудовыми отношениями, то есть субъектов, являющихся работниками данной организации.

По количеству субъектов, ПДн которых обрабатываются, нормативным актом определены 2 категории:

– менее 100000 субъектов;

– более 100000 субъектов.

В ООО «Завод углеродных и композиционных материалов» количество субъектов не превышает 100000 человек.

Последним этапом в установлении уровня защищенности является определение типа угроз актуальных для ИСПДн.

Под актуальными угрозами безопасности ПДн понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного доступа к ПДн при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение ПДн, а также иные неправомерные действия.

Угрозы 1-го типа – угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа – угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа – угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

В соответствии с условиями, указанными в Постановлении Правительства от 1 ноября 2010 г. № 1119, была сформирована таблица 1 для определения уровня защищенности, представленная ниже.

Таблица 1 – Необходимые условия для определения уровня защищенности

Категория	Сотрудники	Количество субъектов	Тип актуальных угроз		
			1	2	3
Специальные	да	Любое	УЗ-1	УЗ-2	УЗ-3
Биометрические	да	Любое	УЗ-1	УЗ-2	УЗ-3
Иные	да	Любое	УЗ-1	УЗ-3	УЗ-4
Общедоступные	да	Любое	УЗ-2	УЗ-3	УЗ-4

Экспертным методом было решено, что угрозы ИСПДн «Бухгалтерия» относятся к 3 типу.

Значит, уровень защищенности ИСПДн «Бухгалтерия» следует считать четвертым.

На данном этапе составляют акт присвоения уровня защищенности ИСПДн «Бухгалтерия», который представлен в приложении Г.

1.6 Вывод по первой главе

После утверждения технического задания было принято решение об аттестации ИСПДн «Бухгалтерия», подготовлена программа и методика аттестационных испытаний, которая определяет, главным образом, перечень работ, порядок, их продолжительность и необходимость использования контрольной аппаратуры.

В ходе проведения обследования объекта информатизации был проведен анализ организационно-распорядительной документации и определен уровень защищенности ИСПДн «Бухгалтерия» согласно Постановлению Правительства от 01.11.2012 г. № 1119 и составлен Акт присвоения уровня защищенности. Рассмотрев исходные данные об информационной системе персональных данных, комиссия определила:

– категория персональных данных: «Иные»;

– количество субъектов персональных данных: менее 100000;

– актуальные угрозы безопасности персональных данных, являются угрозами 3 типа;

– информационной системе персональных данных «Бухгалтерия» Общества с ограниченной ответственностью «Завод углеродных и композиционных материалов» присвоен уровень защищенности: четвертый (УЗ 4).

Установление уровня защищенности ИСПДн необходимо для последующего определения требований к мерам по обеспечению безопасности ПДн.

ГЛАВА 2 РАЗРАБОТКА ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ

2.1 Разработка технической документации

На основе ранее подготовленных документов: опросного листа, Акта обследования (Приложение В) и Акта присвоения УЗ (Приложение Г) был разработан пакет технической документации по защите информации.

Список документации приведен ниже:

– матрица доступа пользователей к защищаемым информационным ресурсам ИСПДн (Приложение Д);

– описание технологического процесса обработки информации в ИСПДн (Приложение Е);

– положение об обработке и защите персональных данных (Приложение Ж).

2.1.1 Матрица доступа пользователей к защищаемым информационным ресурсам ИСПДн

В соответствии с нормативно-методическим документом «СТР-К» для организации была разработана система доступа персонала к сведениям конфиденциального характера[5]. Доступ к информации исполнителей (пользователей, обслуживающего персонала) осуществляется в соответствии с матрицей доступа пользователей к защищаемым информационным ресурсам информационным ресурсам информационной системы персональных данных «Бухгалтерия».

Матрица доступа пользователей к защищаемым ресурсам ИСПДн представлена в приложении Д.

2.1.2 Описание технологического процесса обработки информации в ИСПДн

Описание технологического процесса регламентирует технологию автоматизированной обработки информации в информационной системе персональных данных «Бухгалтерия» Общества с ограниченной ответственностью «Завод углеродных и композиционных материалов».

В документе «Описание технологического процесса обработки информации в ИСПДн» должны быть описаны объекты и субъекты доступа, средства обработки и передачи ПД, схема технологического процесса с привязкой к конкретным средствам обработки и передачи информации.

Описание технологического процесса обработки информации в ИСПДн «Бухгалтерия» представлено в приложении Е.

2.1.3 Положение об обработке и защите персональных данных

В организациях, обрабатывающих ПДн, должен быть документ, который будет отражать политику организации в отношении обработки ПДн – «Положение об обработке и защите персональных данных».

Этот документ определяет:

– принципы обработки ПДн;

– перечень обрабатываемых ПДн;

– цели и способы обработки ПДн;

– категории субъектов, ПДн которых обрабатываются;

– правовое основание обработки ПДн;

– перечень действий с ПДн;

– права и обязанности субъектов ПДн;

– порядок обработки ПД, в том числе хранения, использования и передачи данных;

– условия прекращения обработки ПДн;

– порядок получения доступа к ПДн;

– условия раскрытия и объем ПДн, доступных партнерам и третьим лицам;

– состав и перечень мер по обеспечению защиты ПДн;

– перечень лиц, ответственных за организацию обработки ПДн, его обязанности и формы ответственности.

Положение об обработке и защите персональных данных представлено в приложении Ж.

2.2 Классификация угроз безопасности персональных данных

Для выявления вероятных каналов утечки информации в ИСПДн «Бухгалтерия», нужно разработать частную модель угроз безопасности ПДн, для этого требуется рассмотреть угрозы безопасности, описанные в «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15.02.2008 г.

Состав и содержание угроз безопасности ПДн определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн.

Совокупность таких условий и факторов формируется с учетом характеристик ИСПДн, свойств среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, и возможностей источников угрозы.

Угрозы безопасности ПДн могут быть реализованы за счет утечки ПДн по техническим каналам (технические каналы утечки информации, обрабатываемой в технических средствах ИСПДн, технические каналы перехвата информации при ее передаче по каналам связи, технические каналы утечки акустической (речевой) информации) либо за счет несанкционированного доступа с использованием соответствующего программного обеспечения [8].

Рассмотрим, классификацию угроз утечки информации по техническим каналам.

Основными элементами описания угроз утечки информации по техническим каналам (ТКУИ) являются: источник угрозы, среда (путь) распространения информативного сигнала и носитель защищаемой информации.

Источниками угроз утечки информации по техническим каналам являются физические лица, не имеющие доступа к ИСПДн, а также зарубежные спецслужбы или организации (в том числе конкурирующие или террористические), криминальные группировки, осуществляющие перехват (съем) информации с использованием технических средств ее регистрации, приема или фотографирования.

Среда распространения информативного сигнала – это физическая среда, по которой информативный сигнал может распространяться и приниматься (регистрироваться) приемником. Среда распространения может быть как однородной (например, только воздушной), так и неоднородной за счет перехода сигнала из одной среды в другую (например, в результате акустоэлектрических или виброакустических преобразований).

Носителем ПДн является пользователь ИСПДн, осуществляющий голосовой ввод ПДн в ИСПДн, акустическая система ИСПДн, воспроизводящая ПДн, а также технические средства ИСПДн и ВТСС, создающие физические поля, в которых информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

При обработке ПДн в ИСПДн за счет реализации технических каналов утечки информации возможно возникновение следующих УБПДн:

– угроз утечки акустической (речевой) информации;

– угроз утечки видовой информации;

– угроз утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН).

2.2.1 Угрозы утечки акустической (речевой) информации

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

Перехват акустической (речевой) информации в данных случаях возможен с использованием аппаратуры, регистрирующей акустические (в воздухе) и виброакустические (в упругих средах) волны, а также электромагнитные (в том числе оптические) излучения и электрические сигналы, модулированные информативным акустическим сигналом, возникающие за счет преобразований в технических средствах обработки ПДн, ВТСС и строительных конструкциях и инженерно-технических коммуникациях под воздействием акустических волн[7].

Кроме этого, перехват акустической (речевой) информации возможен с использованием специальных электронных устройств съема речевой информации, внедренных в технические средства обработки ПДн, ВТСС и помещения или подключенных к каналам связи.

Канал утечки для рассматриваемой ИСПДн не актуален.

2.2.2 Угрозы утечки видовой информации

Угрозы утечки видовой информации реализуются за счет просмотра ПДн с помощью оптических (оптикоэлектронных) 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.

Кроме этого, просмотр (регистрация) ПДн возможен с использованием специальных электронных устройств съема, внедренных в служебных помещениях или скрытно используемых физическими лицами при посещении ими служебных помещений. Угрозы безопасности ПДн, связанные с их перехватом при использовании специальных электронных устройств съема видовой информации (видеозакладок), определяются в соответствии с нормативными документами Федеральной службы безопасности Российской Федерации в установленном ею порядке.

Необходимым условием осуществления просмотра (регистрации) ПДн является наличие прямой видимости между средством наблюдения и носителем ПДн.

Канал утечки для рассматриваемой ИСПДн не актуален.

2.2.3 Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок

Возникновение угрозы ПДн по каналам ПЭМИН возможно за счет перехвата техническими средствами побочных (не связанных с прямым функциональным значением элементов ИСПДн) информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПД техническими средствами ИСПДн.

Возникновение угрозы ПДн по каналам ПЭМИН возможно за счет перехвата техническими средствами побочных информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПДн техническими средствами ИСПДн.

По техническому заданию угрозы ПДн по каналам ПЭМИН признаны заказчиком неактуальными, поэтому данные угрозы не рассматривались.

Каналы утечки информации, обусловленные наводками, образуются за счет соединительных линий технических средств ИСПДн и ВТСС и посторонних проводников (в том числе цепей электропитания и заземления).

Наводки электромагнитных излучений технических средств ИСПДн возникают при излучении элементами технических средств ИСПДн информативных сигналов при наличии емкостной, индуктивной или гальванической связей соединительных линий технических средств ИСПДн и линий ВТСС. В результате на случайных антеннах наводится информативный сигнал [7].

Принимая во внимание тот факт, что, линии, расположенные в кабинете Бухгалтерии, где размещена ИСПДн «Бухгалтерия» не выходят за пределы контролируемой зоны, канал утечки информации, обусловленный наводками, не актуален.

Канал утечки для рассматриваемой ИСПДн не актуален.

2.3 Угрозы несанкционированного доступа к информации в информационной системе персональных данных

Угрозы НСД в ИСПДн с применением программных и программно-аппаратных средств реализуются при осуществлении несанкционированного, в том числе случайного, доступа, в результате которого осуществляется нарушение конфиденциальности (копирование, несанкционированное распространение), целостности (уничтожение, изменение) и доступности (блокирование) ПДн, и включают в себя:

– угрозы доступа (проникновения) в операционную среду компьютера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ общего применения);

– угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.п.;

– угрозы внедрения вредоносных программ (программно-математического воздействия).

Источниками угроз НСД в ИСПДн могут быть:

– нарушитель;

– носитель вредоносной программы;

– аппаратная закладка.

Угрозы безопасности ПДн, связанные с внедрением аппаратных закладок, определяются в соответствии с нормативными документами Федеральной службы безопасности Российской Федерации в установленном ею порядке.

По наличию права постоянного или разового доступа в контролируемую зону (КЗ) ИСПДн нарушители подразделяются на два типа:

– нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена, – внешние нарушители;

– нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн, – внутренние нарушители.

Внешними нарушителями могут быть: разведывательные службы государств, криминальные структуры, конкуренты (конкурирующие организации), недобросовестные партнеры, внешние субъекты (физические лица).

Внешний нарушитель имеет следующие возможности:

– осуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений;

– осуществлять несанкционированный доступ через автоматизированные рабочие места, подключенные к сетям связи общего пользования и (или) сетям международного информационного обмена;

– осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;

– осуществлять несанкционированный доступ через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизации, сопровождения, ремонта, утилизации) оказываются за пределами контролируемой зоны;

– осуществлять несанкционированный доступ через информационные системы взаимодействующих ведомств, организаций и учреждений при их подключении к ИСПДн.

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны режимных и организационно-технических мер защиты, в том числе по допуску физических лиц к ПДн и контролю порядка проведения работ.

В «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных» внутренние потенциальные нарушители подразделяются на 8 категорий в зависимости от способа доступа и полномочий доступа к ПДн.

Выявление угроз НСД к ПДн, реализуемых с применением программных и программно-аппаратных средств, осуществляется на основе экспертного метода, в том числе путем опроса специалистов, персонала ИСПДн, должностных лиц, при этом могут использоваться специальные инструментальные средства (сетевые сканеры) для подтверждения наличия и выявления уязвимостей программного и аппаратного обеспечения ИСПДн.

Канал утечки актуален для рассматриваемой ИСПДн.

2.4 Уязвимости информационной системы персональных данных.

Уязвимость информационной системы персональных данных – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечение автоматизированной информационной системы, которые могут быть использованы для реализации угрозы безопасности персональных данных.

Классификация уязвимостей ПО приведена на рисунке 1.

Рисунок 1 – Классификация уязвимостей ПО

Причинами возникновения уязвимостей являются:

– ошибки при проектировании и разработке программного (программно-аппаратного) обеспечения;

– преднамеренные действия по внесению уязвимостей в ходе проектирования и разработки программного (программно-аппаратного) обеспечения;

– неправильные настройки программного обеспечения, неправомерное изменение режимов работы устройств и программ;

– несанкционированное внедрение и использование неучтенных программ с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);

– внедрение вредоносных программ, создающих уязвимости в программном и программно-аппаратном обеспечении; несанкционированные неумышленные действия пользователей, приводящие к возникновению уязвимостей;

– сбои в работе аппаратного и программного обеспечения (вызванные сбоями в электропитании, выходом из строя аппаратных элементов в результате старения и снижения надежности, внешними воздействиями электромагнитных полей технических устройств и др.).

Данная уязвимость актуальна для рассматриваемой ИСПДн.

2.4.1 Уязвимости системного программного обеспечения

Уязвимости системного программного обеспечения необходимо рассматривать с привязкой к архитектуре построения вычислительных систем.

При этом возможны уязвимости:

– в микропрограммах, в прошивках ПЗУ, ППЗУ;

– в средствах операционной системы, предназначенных для управления локальными ресурсами ИСПДн, драйверах, утилитах;

– в средствах операционной системы, предназначенных для выполнения вспомогательных функций, – утилитах, системных обрабатывающих программах, программах предоставления пользователю дополнительных услуг, библиотеках процедур различного назначения;

– в средствах коммуникационного взаимодействия операционной системы.

Уязвимость для рассматриваемой ИСПДн не актуальна.

2.4.2 Уязвимости прикладного программного обеспечения

К прикладному программному обеспечению относятся прикладные программы общего пользования и специальные прикладные программы.

Прикладные программы общего пользования – текстовые и графические редакторы, медиа-программы, системы управления базами данных, программные платформы общего пользования для разработки программных продуктов, средства защиты информации общего пользования и т.п.

Специальные прикладные программы – это программы, которые разрабатываются в интересах решения конкретных прикладных задач в данной ИСПДн.

Уязвимости прикладного программного обеспечения могут представлять собой:

– функции и процедуры, относящиеся к разным прикладным программам и несовместимые между собой (не функционирующие в одной операционной среде) из-за конфликтов, связанных с распределением ресурсов системы;

– функции, процедуры, изменение определенным образом параметров которых позволяет использовать их для проникновения в операционную среду ИСПДн и вызова штатных функций операционной системы, выполнения не-

санкционированного доступа без обнаружения таких изменений операционной системой;

– фрагменты кода программ, введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др., предусмотренные в операционной системе;

– отсутствие необходимых средств защиты (аутентификации, проверки целостности, проверки форматов сообщений, блокирования несанкционированно модифицированных функций и т.п.);

– ошибки в программах (в объявлении переменных, функций и процедур, в кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации, к возможности несанкционированного доступа к информации.

Уязвимость актуальна для рассматриваемой ИСПДн.

2.5 Типовая модель угроз безопасности персональных данных

Согласно типовой модели угроз безопасности ПД, обрабатываемых в локальных информационных системах ПДн, не имеющих подключение к сетям связи общего пользования или сетям международного информационного обмена, при обработке ПДн возможна реализация следующих угроз безопасности ПДн:

– угрозы утечки информации по техническим каналам;

– угрозы НСД к ПДн, обрабатываемым на автоматизированном рабочем месте.

Угрозы утечки информации по техническим каналам включают в себя:

– угрозы утечки акустической (речевой) информации;

– угрозы утечки видовой информации;

– угрозы утечки информации по каналу ПЭМИН.

Возникновение угроз безопасности ПДн в рассматриваемых ИСПДн по техническим каналам характеризуется теми же условиями и факторами, что и для локальных ИСПДн, не имеющих подключения к сетям связи общего пользования и (или) сетям международного информационного обмена.

Угрозы НСД в локальных ИСПДн связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн.

Угрозы НСД в ИСПДн, связанные с действиями нарушителей, имеющих доступ к ИСПДн, аналогичны тем, которые имеют место для отдельного АРМ, не подключенного к сетям связи общего пользования.

Кроме того, в такой ИСПДн могут иметь место:

– угрозы «Анализа сетевого трафика» с перехватом передаваемой по сети информации;

– угрозы выявления паролей;
– угрозы удаленного запуска приложений;
– угрозы внедрения по сети вредоносных программ.

2.6 Разработка частной модели угроз

Первым пунктом в обеспечении безопасности ПДн, согласно ст.19 ФЗ № 152 от 27.07.2006 г. «О персональных данных», является определение угроз безопасности ПДн при их обработке в ИСПДн.

Наличие источника угрозы и уязвимого звена, которое может быть использовано для реализации угрозы, свидетельствует о наличии данной угрозы. Формируя на основе опроса перечень источников угроз ПДн, по данным обследования ИСПДн – перечень технических каналов утечки информации, определяются условия существования в ИСПДн угроз безопасности информации и составляется их полный перечень. На основании этого перечня в соответствии с порядком, описанным в «Методике определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», формируется перечень актуальных угроз безопасности ПДн.

Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет собой опасность для ПДн.

Для оценки возможности осуществления угрозы применяются два показателя:

– уровень исходной защищенности ИСПДн;
– вероятность реализации рассматриваемой угрозы.

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн, приведенных в таблице 2.

Таблица 2 – Показатели исходной защищенности ИСПДн «Бухгалтерия»

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
1 По территориальному размещению:			
Локальная ИСПДн в пределах одного здания	+		
2 По наличию соединения с сетями общего пользования:			
ИСПДн, физически отделенная от сети	+		
3 По встроенным (легальным) операциям с записями баз ПДн:			
Чтение, поиск, запись, удаление, сортировка, модификация, передача			+
4 По разграничению доступа к ПДн:			
Определенный перечень сотрудников		+	
5 По наличию соединений с другими базами ПДн иных ИСПДн:			
С одной БД	+		
6 По уровню обобщения (обезличивания) ПДн:			
Не обезличиваются			+
7 По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:			
Не предоставляется никакой информации	+		
Характеристики ИСПДн	57,14%	14,28%	28,58%
	71,42%		

Так как не менее 70% характеристик соответствуют уровню защищенности не ниже «средний», ИСПДн имеет средний уровень исходной защищенности.

В соответствии с «Методикой…» при составлении перечня актуальных угроз безопасности ПДн для каждой исходной защищенности определяется числовой коэффициент Y_1, а именно:

0 – для высокой степени исходной защищенности;

5 – для средней степени исходной защищенности;

10 – для низкой степени исходной защищенности.

Под вероятностью реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки. Существуют четыре вербальных градации этого показателя:

маловероятно – отсутствуют объективные предпосылки для осуществления угрозы;

низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию;

средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;

высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты.

Каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент Y_2 , а именно:

0 – для маловероятной угрозы;

2 – для низкой вероятности угрозы;

5 – для средней вероятности угрозы;

10 – для высокой вероятности угрозы.

Коэффициент реализуемости угрозы Y будет определяться соотношением

$$Y = (Y_1 + Y_2)/ 20.$$

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

если $0 \le Y \le 0,3$, то возможность реализации угрозы – низкая;

если $0,3 < Y \le 0,6$, то возможность реализации угрозы – средняя;

если $0,6 < Y \le 0,8$, то возможность реализации угрозы – высокая;

если $Y > 0,8$, то возможность реализации угрозы – очень высокая.

Далее оценивается опасность каждой угрозы. При оценке опасности на основе опроса специалиста в области защиты информации определяется вербальный показатель опасности для рассматриваемой ИСПДн. Этот показатель 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.

Затем осуществляется выбор из предварительного перечня угроз безопасности тех, которые относятся к актуальным для данной ИСПДн, в соответствии с правилами, приведенными в таблице 3.

Таблица 3 – Правила отнесения угрозы безопасности к актуальным

Вероятность 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

Так, на основе вышеизложенного порядка определения актуальных угроз безопасности ПДн была разработана частная модель угроз безопасности ПДн при их обработке в ИСПДн «Бухгалтерия», представленная в приложении З.

2.7 Меры по обеспечению безопасности персональных данных

После того, как определены актуальные угрозы, должны быть приняты меры по обеспечению безопасности ПДн для защиты ПД от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн.

Меры по обеспечению безопасности ПДн должны быть реализованы в соответствии с требованиями к защите ПД при их обработке в ИСПДн, утвержденными Постановлением Правительства РФ от 01.11.2012 г. № 1119, а также посредством применения средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия, в случаях, когда применение этих средств необходимо для нейтрализации актуальных угроз безопасности ПДн.

Согласно приказу ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» в состав мер входят следующие направления:

– идентификация и аутентификация субъектов доступа и объектов доступа;

– управление доступом субъектов доступа к объектам доступа;

– ограничение программной среды;

– защита машинных носителей информации, на которых хранятся или обрабатываются ПДн;

– регистрация событий безопасности;

– антивирусная защита;

– обнаружение (предотвращение) вторжений;

– контроль (анализ) защищенности ПДн;

– обеспечение целостности информационной системы и ПДн;

– обеспечение доступности ПДн;

– защита среды виртуализации;

– защита технических средств;

– защита информационной системы, ее средств, систем связи и передачи данных;

– выявление инцидентов, которые могут привести к сбоям или нарушению функционирования информационной системы и к возникновению угроз безопасности ПДн, и реагирование на них;

– управление конфигурацией информационной системы.

Механизм создания набора мер по обеспечению безопасности ПДн, необходимых для конкретной системы состоит из четырех этапов.

Первым этапом является определение базового набора мер по обеспечению безопасности ПДн для установленного уровня защищенности в соответствии с базовыми наборами мер, приведенных в приложении к приказу ФСТЭК № 21.

Вторым этапом является адаптация базового набора мер защиты с учетом целей и задачи обеспечения безопасности информации, структурно-функциональных характеристик информационной системы, информационных технологий.

Третьим этапом служит уточнение адаптированного базового набора мер по обеспечению безопасности ПДн с учетом не выбранных ранее мер. Результатом этого этапа определение мер, направленных на нейтрализацию всех актуальных угроз безопасности для конкретной ИСПДн.

Последним этапом является дополнение уточненного адаптированного базового набора мер по обеспечению безопасности ПДн мерами, обеспечивающими выполнение требований к защите ПДн, установленными нормативными правовыми актами в области обеспечения безопасности ПДн и защиты информации.

Так как для ИСПДн «Бухгалтерия» определен четвертый уровень защищенности, для обеспечения безопасности ПДн должны применяться

– средства вычислительной техники не ниже 6 класса;

– средства защиты информации не ниже 6 класса.

Так, на основе приказа ФСТЭК № 21 разработан документ «Меры по обеспечению безопасности ПДн при их обработке в ИСПДн «Бухгалтерия» (приложение И).

2.8 Модель потенциального нарушителя

В рамках разработки модели нарушителя безопасности персональных данных проводится анализ возможностей, которыми может обладать нарушитель.

На этапах разработки, производства, хранения, транспортировки, ввода в эксплуатацию технических и программных средств криптосредства и СФК обработка персональных данных не производится. Поэтому объектами атак могут быть только сами эти средства и документация на них.

В связи с изложенным на указанных этапах возможны следующие атаки:

– внесение негативных функциональных возможностей в технические и программные компоненты криптосредства и СФК, в том числе с использованием вредоносных программ;

– внесение несанкционированных изменений в документацию на криптосредство и технические и программные компоненты СФК.

Необходимо отметить, что указанные атаки:

– на этапах разработки, производства и транспортировки технических и программных средств криптосредства и СФК могут проводиться только вне зоны ответственности оператора;

– на этапе хранения технических и программных средств криптосредства и СФК могут проводиться как в зоне, так и вне зоны ответственности оператора;

– на этапе ввода в эксплуатацию технических и программных средств криптосредства и СФК могут проводиться в зоне ответственности оператора.

Атака как любое целенаправленное действие характеризуется рядом существенных признаков. К этим существенным признакам на этапе эксплуатации технических и программных средств криптосредства и СФК вполне естественно можно отнести:

– нарушителя - субъекта атаки;

– объект атаки;

– цель атаки;

– имеющуюся у нарушителя информацию об объекте атаки; имеющиеся у нарушителя средства атаки;

– канал атаки.

Описание нарушителей (субъектов атак):

Различают шесть основных типов нарушителей: H1 H2, ..., H6.

Предполагается, что нарушители типа H5 и H6 могут ставить работы по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа криптосредств и СФК.

Возможности нарушителя типа Hj+1 включают в себя возможности нарушителя типа Hi (1 <i <5).

Если внешний нарушитель обладает возможностями по созданию способов и подготовки атак, аналогичными соответствующим возможностям нарушителя типа Hj, то этот нарушитель также будет обозначаться как нарушитель типа Hj.

Нарушители типа H1 и H2 располагают только доступными в свободной продаже аппаратными компонентами криптосредства и СФК.

Дополнительные возможности нарушителей типа Н3-Н5 по получению аппаратных компонент криптосредства и СФК зависят от реализованных в информационной системе организационных мер.

Нарушители типа Н6 располагают любыми аппаратными компонентами криптосредства и СФК.

Уровень криптографической защиты персональных данных, уровни специальной защиты от утечки по каналам побочных излучений и наводок и уровни защиты от несанкционированного доступа.

Различают шесть уровней КС1, КС2, КСЗ, КВ1, КВ2, КА1 криптографической защиты персональных данных, не содержащих сведений, составляющих государственную тайну, определенных в порядке возрастания количества и жесткости предъявляемых к криптосредствам требований, и, соответственно, шесть классов криптосредств, также обозначаемых через КС1, КС2, КСЗ, КВ1, КВ2, КА1.

Уровень криптографической защиты персональных данных, обеспечиваемой криптосредством, определяется оператором путем отнесения нарушителя, действиям которого должно противостоять криптосредство, к конкретному типу.

При отнесении нарушителя к типу Н криптосредство должно обеспечить криптографическую защиту по уровню КС 1, к типу Н2 - КС2, к типу Н3 -КСЗ, к типу Н4 - КВ 1, к типу Н5 - КВ2, к типу Н6 - КА1.

В соответствии с «Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных и конфиденциальной информации при их обработке в автоматизированной системе» была разработана модель потенциального нарушителя ИСПДн «Бухгалтерия» (Приложение К).

2.9 Вывод по второй главе

В ходе данного этапа был разработан пакет технической документации. Была проанализирована базовая модель угроз, на основе которой разработана частная модель угроз безопасности персональных данных при их обработке в ИСПДн «Бухгалтерия». Таким образом, актуальными для ИСПДн «Бухгалтерия» являются следующие угрозы:

– компьютерные вирусы;

– угрозы несанкционированного доступа по каналам связи со стороны нарушителей, не имеющих доступ к ИСПДн;

– угрозы перехвата при передаче по проводным (кабельным) линиям связи;

– угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств.

Также на данном этапе были определены меры по обеспечению безопасности ПДн при их обработке в ИСПДн. На основе «Методических рекомендаций…» разработана Модель потенциального нарушителя ИСПДн «Бухгалтерия».

Основной целью данной главы было выявление актуальных угроз и мер по их устранению.

ГЛАВА 3 ЭТАП АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

3.1 Выбор средств защиты информации

3.1.1 Общие положения

Одним из основных этапов проведения аттестации является проверка полноты и достаточности выбранных мер защиты информации. Все СЗИ, согласно Приказу ФСТЭК № 21 от 18 февраля 2013 г. имеют действующие сертификаты соответствия требованиям безопасности информации.

Технические меры защиты информации реализуются посредством применения средств защиты информации, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности. В данной информационной системе 4 класса защищенности применяются средства защиты информации 6 класса, а также средства вычислительной техники 6 класса.

Выбор СЗИ проводился по нескольким параметрам: стоимость, простота в администрировании, популярность в использовании и иные.

3.1.2 Выбор средства защиты информации от несанкционированного доступа

Выбор средства защиты информации от НСД осуществляется с учетом стоимости, удобства развертывания, знаний обслуживающего персонала и оперативно работающей технической поддержки.

Выбор проводился из трех средств защиты от НСД:

Secret Net 7 (Сертификат ФСТЭК №2707, действителен до 07.09.2018 г.);

Страж NT. Версия 4.0 (Сертификат ФСТЭК №2707, действителен до 20.04.2019 г.);

Dallas Lock 8.0-K. (Сертификат ФСТЭК №2707, действителен до 25.09.2018 г.);

Сравнительный анализ приведен в Таблице 4.

Таблица 4 – Сравнение средств защиты от НСД

Наименование	Стоимость	Наличие документации и техподдержка	Знания обслуживающего персонала (администратора)
Secret Net 7	7 658,05	+	+
Страж NT. Версия 4.0	7 500 р.	+	-
Dallas Lock 8.0-K.	7 500 р.	+	+/-

3.1.3 Выбор средства антивирусной защиты

Следует отметить, что на объекте информатизации ИСПДн «Бухгалтерия» было заранее установлено средство антивирусной защиты «Kaspersky Endpoint Security 10 для Windows». Данное антивирусное средство соответствует требованиям безопасности ФСТЭК России. (Сертификат ФСТЭК России № 3025, действителен до 25.11.2019).

3.1.4 Выбор межсетевого экрана и средства криптографической защиты

Поскольку ООО «Завод углеродных и композиционных материалов» входит в Государственную корпорацию «Росатом», то согласно требованиям, на объекте информатизации должны быть установлены средства криптографической защиты и межсетевого экранирования «Программный комплекс С-Терра Клиент Версия 4.1».

Установленное средство защиты удовлетворяет необходимым требованиям по защите информации и может использоваться на объекте информатизации. Действующие сертификаты приведены в таблице 5.

Таблица 5 – Сведения о сертификатах

Назначение	Сертификат ФСТЭК	Сертификат ФСБ
Соответствует требованиям ФСБ России к шифровальным (криптографическим) средствам класса КС1 и может использоваться для криптографической защиты информации, не содержащей сведений, составляющих государственную тайну. Фильтрация принимаемых и передаваемых пакетов по различным критериям (адресам отправителя и получателя, протоколам, номерам портов, дополнительным полям пакетов и т.д.) в соответствии с требованиями РД.	№ 3371 действителен до 27.03.2021	№ СФ/114-3227 действителен до 15.11.2019

С-Терра Клиент обеспечивает следующие функции:

– защиту трафика на уровне аутентификации/шифрования сетевых пакетов по протоколам IPsec AH и/или IPsec ESP;

– пакетную и контекстную фильтрацию любого исходящего и входящего трафика на хост с использованием информации в полях заголовков сетевого, транспортного и прикладного уровней;

– фильтрацию с учетом входного и выходного сетевого интерфейса;

– фильтрацию запросов на установление виртуальных соединений;

– фильтрацию по любым значимым полям IP-заголовка и полям данных сетевого пакета;

– фильтрацию с учетом даты и времени;

– аутентификацию пользователя и аутентификацию узла сети;

– идентификацию и аутентификацию администратора при доступе с целью администрирования;

– событийное протоколирование;

– реализацию заданной дисциплины взаимодействия (аутентификацию и/или защиту трафика) для каждого защищенного соединения, доступ в заданном защищенном режиме только для зарегистрированных, в том числе и для мобильных партнеров по взаимодействию;

– регулируемую стойкость защиты трафика.

На данном этапе проведения аттестации должны быть разработаны инструкция по эксплуатации средств защиты (приложение Л) и технический паспорт на объект информатизации.

В техническом паспорте описываются основные технические средства и системы (ОТСС), вспомогательные технические средства и системы (ВТСС), средства защиты информации, схемы расположения ОТСС, ВТСС и линий, проложенных в данном помещении.

Технический паспорт представлен в приложении М.

3.2 Аттестационные испытания

Аттестационные испытания ИСПДн проводились в соответствии «Программой и методикой проведения аттестационных испытаний». Аттестационные испытания содержат следующие направления:

– оценка соответствия ИСПДн организационно-техническим требованиям по обеспечению безопасности ПДн;

– оценка соответствия ИСПДн требованиям по защите информации от несанкционированного доступа к ИСПДн.

Оценка соответствия ИСПДн организационно-техническим требованиям по обеспечению безопасности ПД была осуществлена в следующем порядке:

– проверка достаточности представленных документов и соответствия их содержания требованиям по безопасности информации;

– исследование технологического процесса обработки и хранения информации, анализ информационных потоков, определение состава использованных для обработки информации технических средств;

– проверка правильности присвоения уровня защищенности объекта информатизации;

– проверка уровня подготовки кадров и распределения ответственности между персоналом по следующим направлениям;

– проверка наличия сертификатов соответствия на технические средства и средства защиты информации;

– проверка выполнения требований к помещениям, в которых производится обработка информации.

По результатам анализа технологического процесса в соответствии с «Программой и методикой проведения испытаний…» было решено проводить следующие испытания по защите информации от несанкционированного доступа к ИСПДн: подсистем управления доступом; регистрации и учёта, контроля целостности и антивирусной защиты на соответствие требованиям руководящих документов по защите информации.

Испытания проводились специальными средствами проверки:

– программой поиска и гарантированного уничтожения информации на дисках «TERRIER»;

– программой фиксации и контроля исходного состояния программного комплекса «ФИКС»;

– средством создания модели системы разграничения доступа «Ревизор 1 XP»;

– программой контроля полномочий доступа к информационным ресурсам «Ревизор 2XP»;

– программой поиска и контроля уязвимостей в вычислительных сетях «Ревизор сети 3.0».

По результатам оценки было оформлено заключение. В заключение включены протоколы, подтверждающие полученные при оценке результаты и обосновывающие приведенный в заключении вывод.

Заключение по результатам аттестационных испытаний представлено в приложении Н.

3.3 Оценка экономической эффективности проекта

В результате предпроектного обследования были выявлены уязвимости, которые подлежат устранению. Данные проблемы возможно устранить с помощью создания комплексной системы защиты информации. Для этого необходимо произвести расчёт экономической эффективности проекта, который ответит на вопрос о целесообразности реализации мер по созданию комплексной системы защиты информации. Стоимость программных и технических средств представлена в таблице 6. Стоимость услуг по реализации проекта представлена в таблице 7. Поток денежных платежей представлен в таблице 8.

Таблица 6 – стоимость обеспечения

№ п/п	Наименование	Количество (шт.)	Цена за шт. (руб.)	Сумма (руб.)
1	Secret Net 7	1	7 658	7 658
2	С-Терра Клиент. Версия 4.1	1	4 600	4 600
3	Kaspersky Стартовый Certified Media Pack	1	500	500
Итог				12 758

Таблица 7 – стоимость услуг по обеспечению проекта

№ п/п	Наименование	Стоимость (руб.)
1	Обследование автоматизированной системы	2 119
2	Разработка комплекта ОРД согласно отраслевым требованиям ГК «Росатом» и требованиям законодательства в сфере обработки и защиты персональных данных с учетом требований к ОРД	3 814
3	Разработка технического проекта системы защиты конфиденциальной информации в АСЗИ	3 178
4	Проведение работ по установке и настройке средств защиты информации	2 966
5	Проведение инструментального анализа защищенности	1 060
6	Разработка комплекта документов, необходимых для представления АСЗИ предприятия к аттестации на соответствие требованиям безопасности информации по классу защищенности автоматизированных систем класса 2Б	4 279
7	Проведение обучения специалистов Заказчика по администрированию поставляемых средств защиты информации	1 695
8	Проведение аттестации АСЗИ организации по классу защищенности 2Б	7 082
Итог		19 201

Стоимость внедрения СЗИ в ООО «Завод углеродных и композиционных материалов» составляет 31959.

Таблица 8 – поток денежных платежей по проекту

Периоды	0	1	2	3
Первоначальные инвестиции (руб.)	-31 959			
Выгоды (размеры риска) (руб.)		300 000	300 000	300 000
Стоимость годовой поддержки (руб.)		-5 000	-5 000	-5 000
Затраты на администрирование и инфраструктуру (руб.)		-10 000	-10 000	-10 000
Итого	-31 959	298 500	298 500	298 500

Денежные вложения в реализацию проекта комплексной системы защиты информации составляют 31959 рублей. Ежегодно для поддержания системы необходимо выделять по 15000 рублей, на протяжении трех лет. Для наглядного показа отличия вложений средств в проект от дохода хранения денег в банке воспользуемся методом Net Present Value (NPV). Рассчитаем NPV по формуле:

$$NPV = \sum_{t=1}^{n} \frac{CF_t}{(1+r)^t} - \sum_{t=0}^{n} \frac{I_t}{(1+r)^t}$$

Где CF – денежный поток;

I – сумма инвестиционных вложений в проект в t-ом периоде;

r – ставка дисконтирования;

n – количество периодов.

Значение финансовых поступлений будем считать равным размеру ставки Центробанка России. Ставка центрального банка составляет 7,25 %

$$NPV = -31959 + \frac{298500}{1.0725} + \frac{298500}{1.0725^2} + \frac{298500}{1.0725^3} =$$

$$= -31959 + 277674.42 + 258301.78 + 258301.78 = 762318.95$$

Из произведенного расчета видно, что значение NPV больше 0. Таким образом, в данной организации будет целесообразным проект внедрения СЗИ. На основании вышесказанного можно сделать вывод, что создание СЗИ в данной организации будет эффективным, так как величина потерь при отсутствии реализованных мер будет превышать затраты на ее реализацию и обслуживание.

3.4 Вывод по третьей главе

На данном этапе был произведен выбор средств защиты информации для данной ИСПДн. Проведены аттестационные испытания, в ходе которых аттестационная комиссия посчитала, что реализованные средства и меры защиты достаточны и соответствуют требованиям действующих нормативных документов по безопасности информации. Таким образом, на аттестуемую ИСПДн «Бухгалтерия» был выдан аттестат соответствия на право обработки ПДн в соответствии с установленным уровнем защищенности и сроком на три года (приложение У).

Проведена экономическая эффективность проекта, по результатам которой можно сделать вывод об экономической целесообразности внедрения средств защиты информации.

ГЛАВА 4 БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

4.1 Общие положения

При проведении аттестации сотрудникам АО «Гранит Информ» необходимо взаимодействовать с ПЭВМ для ввода, обработки, передачи и хранения информации о результатах аттестационных испытаний, что накладывает определенные требования к персональным компьютерам и помещениям, в которых происходит работа с ПЭВМ: пожарные требования, требования к климату и требования при работе с электроаппаратурой.

В Российской Федерации, нормативно-правовыми актами, регулирующими данный вопрос, являются:

– «Трудовой кодекс Российской Федерации» № 197-ФЗ от 30.12.2001 г.,

– «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы» (СанПиН 2.2.2/2.4.1340-03),

– «Типовая инструкция по охране труда при работе на персональном компьютере» (ТОИ Р-45-084-01).

Государственными нормативными требованиями охраны труда устанавливаются правила, процедуры, критерии и нормативы, направленные на сохранение жизни и здоровья работников в процессе трудовой деятельности.

Статья 209 ТК РФ формулирует основные понятия, используемые при обеспечении охраны труда.

Таблица 9 – Время регламентированных перерывов при работе с ПЭВМ

Категория работы с ПЭВМ	Уровень нагрузки за рабочую смену при видах работы с ПЭВМ по группам			Суммарное время регламентированных перерывов, мин	
	А количество знаков	Б количество знаков	В часов	при 8-часовой смене	при 12-часовой смене
I	до 20 000	до 15 000	до 2,0	30	70
II	до 40 000	до 30 000	до 4,0	50	90
III	до 60 000	до 40 000	до 6,0	70	120

Вредными факторами могут быть:

– физические факторы - температура, влажность, скорость движения воздуха, тепловое излучение, электромагнитные поля (ЭМП) и излучения, производственный шум, вибрация, аэрозоли, освещение - естественное, искусственное;

– химические факторы - химические вещества, смеси;

– биологические факторы - микроорганизмы, живые клетки и споры;

– факторы трудового процесса. [14]

При эксплуатации персонального компьютера на работника могут оказывать действие следующие опасные и вредные производственные факторы:

– повышенное значение напряжения в электрической сети, замыкание которой может привести к поражению электрическим током;

– повышенный уровень напряженности электромагнитного поля;

– пониженный или повышенный уровень освещенности;

– не соответствующие нормам параметры микроклимата;

– повышенный уровень шума. [12]

4.2. Требования к помещениям для работы с ПЭВМ

Перечень продукции и контролируемых гигиенических параметров вредных и опасных факторов представлены в Таблице 10.

Временные допустимые уровни электромагнитных полей, создаваемых ПЭВМ, а также допустимые визуальные параметры устройств отображения информации не должны превышать значений, указанных в СанПиН 2.2.2/2.4.1340-03.

Таблица 10 – Используемая продукция при аттестации

Вид продукции	Код ОКП	Контролируемые гигиенические параметры
Машины вычислительные электронные цифровые, машины вычислительные электронные цифровые персональные (включая портативные ЭВМ)	40 1300	Уровни электромагнитных полей (ЭМП), акустического шума, концентрация вредных веществ в воздухе, визуальные показатели ВДТ
Устройства периферийные: принтеры, сканеры, модемы, сетевые устройства, блоки бесперебойного питания и т.д.	40 3000	Уровни ЭМП, акустического шума, концентрация вредных веществ в воздухе
Устройства отображения информации	40 3200	Уровни ЭМП, визуальные показатели, концентрация вредных веществ в воздухе

Временные допустимые уровни электромагнитных полей, создаваемых ПЭВМ, а также допустимые визуальные параметры устройств отображения информации не должны превышать значений, указанных в СанПиН 2.2.2/2.4.1340-03.

При размещении рабочих мест с ПЭВМ расстояние между рабочими столами с видеомониторами (в направлении тыла поверхности одного видеомонитора и экрана другого видеомонитора), должно быть не менее 2,0 м, а расстояние между боковыми поверхностями видеомониторов – не менее 1,2 м. [10]

Рабочая мебель для пользователей компьютерной техникой должна отвечать следующим требованиям:

– высота рабочей поверхности стола должна регулироваться в пределах 680 - 800 мм; при отсутствии такой возможности высота рабочей поверхности стола должна составлять 725 мм;

– рабочий стол должен иметь пространство для ног высотой не менее 600 мм, глубиной на уровне колен не менее 450 мм и на уровне вытянутых ног не менее 650 мм;

– рабочий стул (кресло) должен быть подъемно - поворотным и регулируемым по высоте и углам наклона сиденья и спинки, а также - расстоянию спинки от переднего края сиденья;

– рабочее место должно быть оборудовано подставкой для ног, имеющей ширину не менее 300 мм, глубину не менее 400 мм, регулировку по высоте в пределах до 150 мм и по углу наклона опорной поверхности подставки до 20 градусов; поверхность подставки должна быть рифленой и иметь по переднему краю бортик высотой 10 мм.[16]

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

Площадь на одно рабочее место пользователей ПЭВМ должна составлять не менее 4,5 м^2.

Клавиатуру следует располагать на поверхности стола на расстоянии 100 - 300 мм от края, обращенного к пользователю, или на специальной регулируемой по высоте рабочей поверхности, отделенной от основной столешницы. [10]

Естественное и искусственное освещение должно соответствовать требованиям действующей нормативной документации. Окна в помещениях, где эксплуатируется вычислительная техника, преимущественно должны быть ориентированы на север и северо-восток.

Оконные проемы должны быть оборудованы регулируемыми устройствами типа: жалюзи, занавесей, внешних козырьков и др.

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

Помещения, где размещаются рабочие места с ПЭВМ, должны быть оборудованы защитным заземлением (занулением) в соответствии с техническими требованиями по эксплуатации.

4.3. Требования к микроклимату, уровню шума и освещению

В производственных помещениях должны обеспечиваться оптимальные параметры микроклимата в соответствии с нормативами микроклимата производственных помещений (СанПиН 2.2.4.3359-16).

Показателями, характеризующими микроклимат в производственных помещениях, являются:

1) температура воздуха;

2) температура поверхностей;

3) относительная влажность воздуха;

4) скорость движения воздуха;

5) интенсивность теплового облучения.

Оптимальные величины параметров микроклимата на рабочих местах применительно к выполнению работ категории 1а в холодный и теплый периоды года приведены в Таблице 11. [15] В помещениях, оборудованных ПЭВМ, проводится ежедневная влажная уборка и систематическое проветривание после каждого часа работы на ПЭВМ. [10]

Таблица 11 – Оптимальные величины параметров микроклимата

Период года	Температура воздуха, ^{0}C	Температура поверхностей, ^{0}C	Относительная влажность воздуха, %	Скорость движения воздуха, м/с, не более
Холодный	22-24	21-25	60-40	0,1
Теплый	23-25	22-26	60-40	0,1

По характеру спектра шума выделяют:

1) тональный шум;

2) широкополосный шум, не содержащий выраженных тонов.

По временным характеристикам шума выделяют:

1) постоянный шум;

2) непостоянный шум, уровень звука которого за 8-часовой рабочий день изменяется более чем на 5 дБА;

3) импульсный шум. [15]

Основными источниками шума в помещениях, оборудованных вычислительной техникой, являются принтеры, плоттеры, копировальные аппараты и оборудование для кондиционирования воздуха, вентиляторы систем охлаждения, трансформаторы.

Нормативным эквивалентным уровнем звука на рабочих местах, согласно СанПиН 2.2.4.3359-16, является 80 дБА. [15]

Рабочие места, оборудованные ПЭВМ, должны быть обеспечены как искусственным, так и естественным светом.

Рабочие столы следует размещать таким образом, чтобы мониторы ПЭВМ были ориентированы боковой стороной к световым проемам, а естественный свет падал преимущественно слева.

Искусственное освещение в помещениях для эксплуатации ПЭВМ для проведения работ по аттестации должно осуществляться системой комбинированного освещения (к общему освещению дополнительно устанавливаются светильники местного освещения, предназначенные для освещения зоны расположения документов).

Освещенность на поверхности стола в зоне размещения рабочего документа должна быть 300-500 лк. Освещение не должно создавать бликов на поверхности экрана. Освещенность поверхности экрана не должна быть более 300 лк.

Следует ограничивать прямую блёскость от источников освещения (не более 200 кд/м^2), а также отраженную блёскость на рабочих поверхностях (не более 40 кд/м^2). Яркость потолка не должна превышать 200 кд/м^2.

Яркость светильников общего освещения должна составлять не более 200 кд/м^2, защитный угол светильников должен быть не менее 40^0.

Применение светильников без рассеивателей и экранирующих решеток не допускается.

Общее освещение при использовании люминесцентных светильников следует выполнять в виде сплошных или прерывистых линий светильников, расположенных сбоку от рабочих мест, параллельно линии зрения пользователя при рядном расположении мониторов. При периметральном расположении компьютеров линии светильников должны располагаться локализовано над рабочим столом ближе к его переднему краю, обращенному к оператору.

Для обеспечения нормируемых значений освещенности в помещениях для использования ПЭВМ следует проводить чистку стекол оконных рам и светильников не реже двух раз в год и проводить своевременную замену перегоревших ламп. [10]

4.4. Обеспечение пожарной и электробезопасности

Степень опасного и вредного воздействия на человека электрического тока, электрической дуги и электромагнитных полей зависит от:

– рода и величины напряжения и тока;

– частоты электрического тока;

– пути тока через тело человека;

– продолжительности воздействия электрического тока или электромагнитного поля на организм человека;

– условий внешней среды.

Электробезопасность должна обеспечиваться:

– конструкцией электроустановок;

– техническими способами и средствами защиты;

– организационными и техническими мероприятиями.

Электроустановки и их части должны быть выполнены таким образом, чтобы работающие не подвергались опасным и вредным воздействиям электрического тока и электромагнитных полей, и соответствовать требованиям электробезопасности.

Для обеспечения защиты от случайного прикосновения к токоведущим частям необходимо применять следующие способы и средства:

– защитные оболочки;

– защитные ограждения (временные или стационарные);

– защитные барьеры;

– безопасное расположение токоведущих частей;

– изоляция токоведущих частей (основная, дополнительная, усиленная, двойная);

– изоляция рабочего места;

– малое напряжение;

– защитное отключение;

– электрическое разделение;

– предупредительная сигнализация, блокировки, знаки безопасности.

Технические способы и средства применяют раздельно или в сочетании друг с другом так, чтобы обеспечивалась оптимальная защита при нормальном функционировании электроустановок и при возникновении аварийных ситуаций.[17]

Сформулирован ряд требований к работе за ПЭВМ с целью обеспечения электробезопасности.

Пред началом работ:

– проверить правильность подключения оборудования к электросети;

– проверить исправность проводов питания и отсутствие оголенных участков проводов;

– убедиться в наличии заземления системного блока, монитора и защитного экрана;

– протереть антистатической салфеткой поверхность экрана монитора и защитного экрана.

Во время работы запрещается:

– прикасаться к задней панели системного блока (процессора) при включенном питании;

– переключать разъемы интерфейсных кабелей периферийных устройств при включенном питании;

– допускать попадание влаги на поверхность системного блока (процессора), монитора, рабочую поверхность клавиатуры, дисководов, принтеров и других устройств;

– производить самостоятельное вскрытие и ремонт оборудования;

– работать на компьютере при снятых кожухах;

– отключать оборудование от электросети и выдергивать электровилку, держась за шнур.

Требования безопасности в аварийных ситуациях:

– Во всех случаях обрыва проводов питания, неисправности заземления и других повреждений, появления гари, немедленно отключить питание и сообщить об аварийной ситуации руководителю.

– Не приступать к работе до устранения неисправностей.

– При получении травм или внезапном заболевании немедленно известить своего руководителя, организовать первую доврачебную помощь или вызвать скорую медицинскую помощь. [16]

Помещение, в котором располагается ПЭВМ, должно иметь систему обеспечения пожарной безопасности с целью предотвращение пожара, обеспечения безопасности людей и защиты имущества при пожаре.

Возможными классам пожаров при работе с ПЭВМ могут быть:

– А – пожары твердых горючих веществ и материалов (огнетушащие вещества: вода, пена, порошок, углекислота);

– В – пожары горючих жидкостей или плавящихся твердых веществ и материалов (пена, порошок, асбестовое полотно, песок, огнетушащие составы на основе фтора и брома для ингибирования);

– Е – пожары горючих веществ и материалов электроустановок, находящихся под напряжением (углекислота, хладон, порошки, вода и пена, если оборудование обесточено);

К опасным факторам пожара, воздействующим на людей и имущество, относятся:

– пламя и искры;

– тепловой поток;

– повышенная температура окружающей среды;

– повышенная концентрация токсичных продуктов горения и термического разложения;

– пониженная концентрация кислорода;

– снижение видимости в дыму.

Защита людей и имущества от воздействия опасных факторов пожара и (или) ограничение последствий их воздействия обеспечиваются одним или несколькими из следующих способов:

1) применение объемно-планировочных решений и средств, обеспечивающих ограничение распространения пожара за пределы очага;

2) устройство эвакуационных путей, удовлетворяющих требованиям безопасной эвакуации людей при пожаре;

3) устройство систем обнаружения пожара (установок и систем пожарной сигнализации), оповещения и управления эвакуацией людей при пожаре;

4) применение систем коллективной защиты (в том числе противодымной) и средств индивидуальной защиты людей от воздействия опасных факторов пожара;

5) применение огнестойких строительных конструкций;

6) применение огнезащитных составов;

7) применение первичных средств пожаротушения;

8) применение автоматических и (или) автономных установок пожаротушения;

9) организация деятельности подразделений пожарной охраны. [10]

4.5 Сравнение требуемых параметров к рабочему месту

Для того, чтобы проверить соответствие условий труда требованиям нормативным документам необходимо провести сравнительный анализ требований, установленных к рабочим местам, оборудованным ПЭВМ и фактических параметров рабочего места. Схема размещения рабочего места приведена на рисунке 2. Площадь помещения 20 м^2. В помещении присутствует естественное и искусственное освещение.

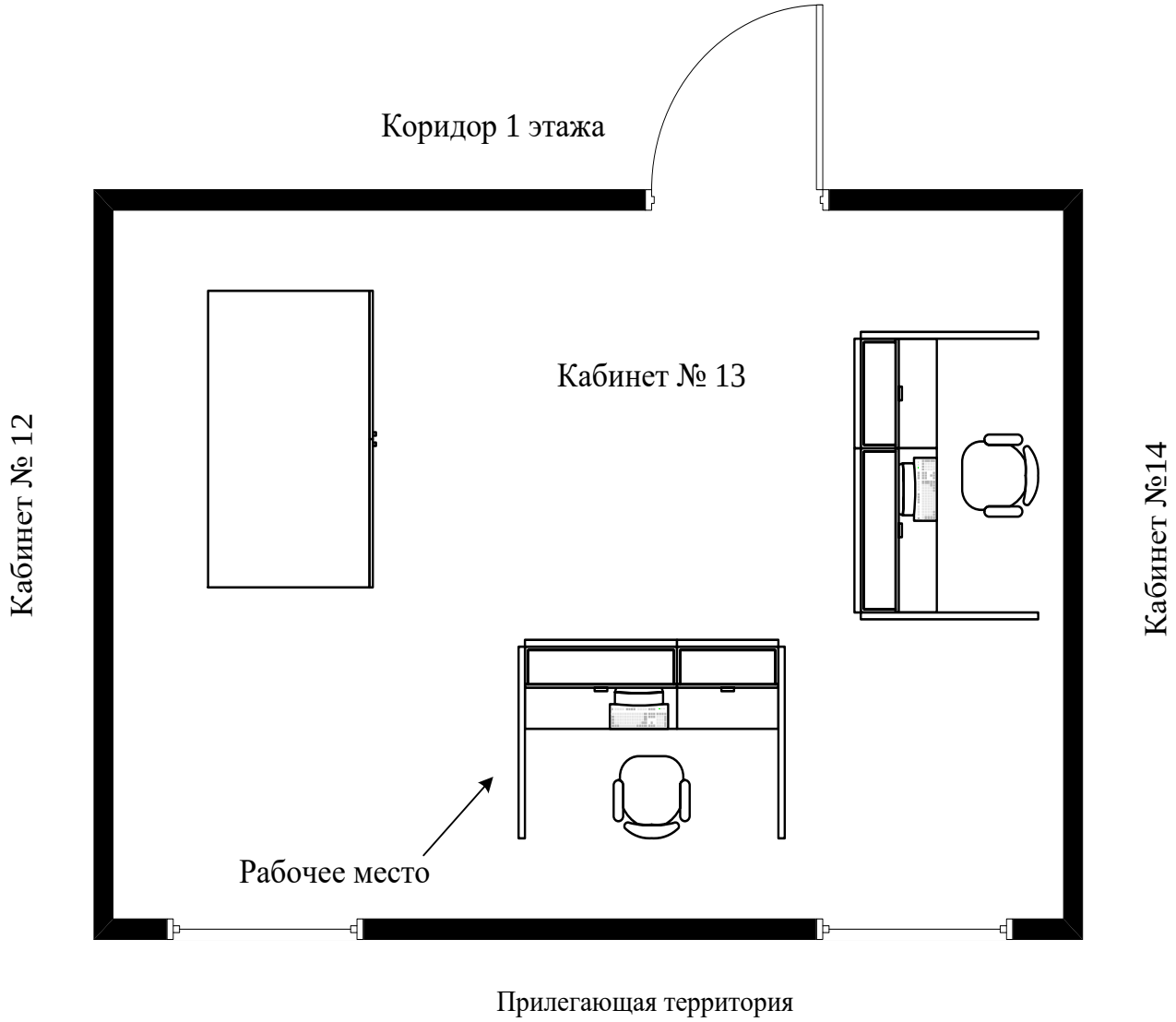

Рисунок 2 – Схема рабочего места

Перечень нормируемых параметров для рабочего места, сравнение их допустимых нормы и фактические значений на рабочем месте представлены в таблице 12.

Таблица 12 – Сравнение параметров рабочего места с допустимыми нормами

Нормируемые параметры	Требуемые значения	Фактические значения
Требования к помещениям		
Высота рабочей поверхности стола	680 - 800 мм, либо 725	748 мм
Пространство для ног	Высота не менее 600 мм; Глубина на уровне колен не менее 450 мм; На уровне вытянутых ног не менее 650 мм.	757 мм 526 мм 680 мм

Нормируемые параметры	Требуемые значения	Фактические значения
Рабочий стул	Должен быть подъемно - поворотным и регулируемым по высоте и углам наклона сиденья и спинки, а также - расстоянию спинки от переднего края сиденья.	Соответствует требованиям
Рабочее место	Должно быть оборудовано подставкой для ног.	Не соответствует требованиям
Экран монитора	Экран должен находиться от глаз пользователя на расстоянии 600-700 мм, но не ближе 500 мм.	670 мм
Площадь рабочего места	Не менее 4,5 $м^2$	8 $м^2$
Клавиатура	Следует располагать на поверхности стола на расстоянии 100 - 300 мм от края, обращенного к пользователю, или на специальной регулируемой по высоте рабочей поверхности, отделенной от основной столешницы.	255 мм
Окна и оконные проемы	Окна преимущественно должны быть ориентированы на север и северо-восток. Оконные проемы должны быть оборудованы регулируемыми устройствами.	Не соответствует требованиям
Требования к микроклимату, уровню шума и освещению		
Температура воздуха	В холодный период 22-24^{0}С В теплый период 23-25^{0}С	23^{0}С
Уровень звука	80 дБА	60 дБА
Освещенность	300-500 лк	330 лк
Обеспечение пожарной и электробезопасности		
Электробезопасность	Электроустановки и их части должны быть выполнены таким образом, чтобы работающие не подвергались опасным и вредным воздействиям электрического тока и электромагнитных полей, и соответствовать требованиям электробезопасности	Соответствует требованиям
Пожарная безопасность	Помещение, в котором располагается ПЭВМ, должно иметь систему обеспечения пожарной безопасности с целью предотвращение пожара, обеспечения безопасности людей и защиты имущества при пожаре.	Соответствует требованиям

4.6 Выводы по четвертой главе

В данном разделе были рассмотрены вредные производственные факторы, которые могут стать угрозой безопасности проведения работ по аттестации объектов информатизации сотрудниками АО «Гранит Информ». Для данных факторов были приведены допустимые значения, установленные нормами СанПин, а также меры по снижению негативного влияния вредных факторов на организм человека.

Были выявлены общие требования к организации рабочих мест пользователей, требования к помещениям для работы с ПЭВМ, основные требования к освещению на рабочих местах, уровню шума и микроклимату. На основе проведенного анализа было установлено, что условия труда на рабочем месте соответствуют вышеперечисленным требованиям за исключением наличия подставки для ног.

ЗАКЛЮЧЕНИЕ

В результате выполнения выпускной квалификационной работы было проведено обследование объекта информатизации ИСПДн «Бухгалтерия» ООО «Завод углеродных и композиционных материалов». Данная ИСПДн обрабатывает ПДн сотрудников. В ходе обследования был проведен анализ организационно-распорядительных документов.

В ходе проведения аттестации был установлен уровень защищенности ИСПДн «Бухгалтерия» и разработана техническая документация: частная модель угроз, описание технологического процесса, матрица доступа и др. В соответствии с установленным уровнем защищенности и актуальными угрозами было выявлено, что данная ИСПДн недостаточно защищена от угроз. Поэтому на объект информатизации было дополнительно установлены средства защиты информации, которые выполняют требования к мерам по обеспечению безопасности информации. В связи с этим был разработан технический паспорт и инструкция по эксплуатации средств защиты информации.

В ходе выполнения выпускной квалификационной работы были проведены аттестационные испытания на соответствия требованиям безопасности информации. В результате было принято решение о выдаче аттестата соответствия ИСПДн «Бухгалтерия» ООО «Завод углеродных и композиционных материалов» на право обработки ПД.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1) «Положение по аттестации объектов информатизации по требованиям безопасности информации» от 25.11.1994 // КонсультантПлюс: Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2017.

2) «Об утверждении доктрины информационной безопасности Российской Федерации»: указ Президента Российской Федерации от 05.12.2016 № 646 // КонсультантПлюс: Интернет-версия [Электронный ресурс] / ЗАО «Консультант». – Электрон. дан. и прогр. – М., 2017.

3) «О персональных данных»: федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ: (в ред. 22.02.2017 г.) // КонсультантПлюс: Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2017.

4) «Об утвержении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных»: приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 23.03.2017 г.) // КонсультантПлюс : Интернетверсия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2017.

5) «Специальные требования и рекомендации по технической защите конфиденциальной информации» от 02.03.2001 № 7.2 //
http://www.rfcmd.ru/sphider/docs/InfoSec/RD_FSTEK_requirements.htm

6) «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»: постановление Правительства Российской Федерации от 01.11.2012 № 1119 // КонсультантПлюс : Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2017.

7) «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15.02.2008 // КонсультантПлюс: Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2017.

8) «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 14.02.2008 // КонсультантПлюс: Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2017.

9) «Защита от несанкционированного доступа к информации Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей»: руководящий документ (Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. № 114) // ФСТЭК: Ин-

тернет-версия [Электронный ресурс] / http://fstec.ru/component/attachments/download/294

10) СанПиН 2.2.2/2.4.1340-03. Гигиенические требования к персональным электронно-вычислительным машинам и организации работы: санитар.-эпидемиол. правила и нормативы: утв. 24.07.03: введ. в д. 30.07.03. – Москва: [б. и.], 2003. – 24 с.

11) О техническом регулировании [Текст]: федер. закон от 27.12.2002 г. № 184-ФЗ // Собр. законодательства РФ. - 2002. - № 52 (ч. 1). - ст. 5140.

12) ГОСТ 12.0.003-2015 Система стандартов безопасности труда (ССБТ). Опасные и вредные производственные факторы. Классификация. – М.: Стандартинформ, 2016. – 16 с.

13) Трудовой кодекс Российской Федерации [Текст]: федер. конституц. закон от 30.12.2001 г. № 197-ФЗ // Собрание законодательства РФ – 2002. – № 1 (1 ч.). – ст. 3.

14) СанПиН 2.2.4.3359-16. Санитарно-эпидемиологические требования к физическим факторам на рабочих местах: санитар.-эпидемиол. правила и нормативы: утв. 21.06.16 г.: введ. в д. 01.01.17. – Москва: [б. и.], 2016. – 24 с.

15) ГОСТ Р 12.1.019-2009 Система стандартов безопасности труда (ССБТ). Электробезопасность. Общие требования и номенклатура видов защиты. – М.: Стандартинформ, 2010. – 27 с.

ПРИЛОЖЕНИЕ А

Техническое задание

на выполнение работ по проведению аттестации объекта информатизации

ООО «Завод углеродных и композиционных материалов»

(далее – техническое задание)

1. Наименование выполняемых работ.

Проведение аттестации объекта информатизации по требованиям безопасности информации.

2. Цель выполнения работ.

Целью выполнения работ является подготовка объекта информатизации к аттестационным испытаниям и проведение аттестационных испытаний объекта информатизации на соответствие требованиям по безопасности информации.

3. Основания выполнения работ.

Федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»;

Постановление Правительства Российской Федерации от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» и другие нормативно-методические и руководящие документы регуляторов, осуществляющих надзор и контроль за выполнением требований безопасности информации.

4. Требования по безопасности информации.

Объект информатизации должен отвечать требованиям информационной безопасности, предъявляемым к объекту, в том числе:

− по порядку и организации работ по защите информации на объекте информатизации;

− по защите информации от утечки за счет наводок;

− по защите информации от утечки по сетям электропитания и заземления;

− по защите информации от утечки за счет НСД;

− по защите информации от утечки за счет предотвращение вредоносных или нежелательных соединений компьютера в локальной сети или сети Интернет.

5. Требования к наличию лицензий. Исполнитель должен иметь следующие лицензии.

− лицензия ФСТЭК России на право осуществлять деятельность по технической защите конфиденциальной информации;

− лицензия ФСТЭК России по разработке и производству средств защиты конфиденциальной информации;

− лицензия ФСБ России на осуществление деятельности по техническому обслуживанию шифровальных (криптографических) средств; или лицензии ФСБ России на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств.

6. Требования к гарантийному сроку и (или) объему предоставления гарантий качества работы.

Требования к гарантийному сроку и (или) объему предоставления гарантий качества работы: 12 месяцев с момента подписания акта выполненных работ.

Ведомость объемов работ

№	Наименование работ
1	Обследование объектов информатизации с определением класса и актуальных угроз безопасности персональных данных при их обработке
2	Разработка проектов организационно-распорядительных документов по защите персональных данных при их обработке для организации, разработка «Модели угроз безопасности персональных данных при их обработке», разработка программы и методики аттестационных испытаний
3	Настройка и установка новых средств и систем защиты информации от несанкционированного доступа к информации, в случае несоответствия требованиям
4	Проведение аттестационных испытаний объектов информатизации в соответствии с уровнем защищенности ИСПДн и нормативно-методическими документами ФСТЭК России и ФСБ России с оформлением «Заключения» и выдачей «Аттестата соответствия» по требованиям безопасности персональных данных

7. Перечень нормативно-правовых документов, используемых Исполнителем при оказании услуг по аттестации ИСПДн «Бухгалтерия»:

Федеральный закон Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральный закон Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

Постановление Правительства РФ от 03.02.2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации»;

Нормативно-методический документ «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утвержден приказом Гостехкомиссии России от 30.08.2002 г. № 282;

«Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные постановлением Правительства от 01.11.2012 г. № 1119.

«Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденные приказом ФСТЭК от 18.02.2013 г. № 21;

Руководящий документ. «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации», утвержден решением председателя Гостехкомиссии России от 30.03.1992 г.;

Руководящий документ. «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации», утвержден решением председателя Гостехкомиссии России от 30.03.1992 г.;

Руководящий документ. «Защита от несанкционированного доступа. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей». Утвержден приказом Председателя Гостехкомиссии России от 04.06.1999 г. № 114;

Руководящий документ. «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» утвержден решением Председателя Гостехкомиссии России 25.07.1997 г.;

«Требования к системам обнаружения вторжений». Утверждены приказом ФСТЭК России от 06.12.2011 г. №638;

«Требования к средствам антивирусной защиты». Утверждены приказом ФСТЭК России от 20.03.2012 г. № 28;

ГОСТ Р 34.602-89 «Техническое задание на создание автоматизированной системы»;

ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;

ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»;

ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения»;

ГОСТ Р 53131-2008 «Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения»;

ГОСТ Р 51583-2000. «Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения»;

ГОСТ Р 51624-2000. «Защита информации. Автоматизированные системы в защищённом исполнении. Общие требования»;

ГОСТ РО 0043-003-2012. Защита информации. Аттестация объектов информатизации. Общие положения.

ГОСТ РО 0043-004-2013. Защита информации. Аттестация объектов информатизации. Программа и методика аттестационных испытаний;

«Положение о сертификации средств защиты информации по требованиям безопасности информации, утверждено» Приказом Гостехкомиссии РФ от 27.10.1995 г. № 199.

8. Дополнительные условия.

8.1. Заказчик в процессе выполнения работ обязан:

-обеспечить доступ представителей Исполнителя на объект Заказчика для выполнения работ, предусмотренных настоящим техническим заданием;

-предоставить необходимую техническую документацию на время выполнения работ.

8.2. Исполнитель в процессе выполнения работ обязан:

-обеспечить соблюдение его представителями требований режима секретности, установленных на объекте Заказчика;

-выполнение всех работ на объекте Заказчика согласовывать с представителем Заказчика;

-представить справку о наличии допуска к сведениям, составляющих государственную тайну и предписание на выполнение работ.

8.3. Срок выполнения работ: в течение 20 дней с момента заключения муниципального контракта.

ПРИЛОЖЕНИЕ Б

Орган по аттестации объектов информатизации по требованиям безопасности информации
(аттестат аккредитации № СЗИ RU.1960.В167.326)

СОГЛАСОВАНО

Исполнительный директор Общества с ограниченной ответственностью «Завод углеродных и композиционных материалов»

_____ С.А. Подкопаев

«_____»_____ 2018 г.

УТВЕРЖДАЮ

Руководитель органа по аттестации объектов информатизации
АО «Гранит Информ»

_____Н.В. Узбеков

«_____»_____ 2018 г.

ПРОГРАММА И МЕТОДИКА

проведения аттестационных испытаний
информационной системы персональных данных
«Бухгалтерия»
Общества с ограниченной ответственностью
«Завод углеродных и композиционных материалов»
на соответствие требованиям по обеспечению безопасности персональных данных

2018

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящий документ определяет цели, задачи, методы, условия, объем, порядок и методики проведения аттестационных испытаний информационной системы персональных данных – «Бухгалтерия» Общества с ограниченной ответственностью «Завод углеродных и композиционных материалов» (далее ИСПДн) на соответствие требованиям по обеспечению безопасности персональных данных. Состав ИСПДн приведён в таблице 1.1.

Таблица 1.1 – **Состав ОТСС**

№ П/П	Наименование технического средства	Модель	Заводской (инвентарный) номер
1.	Системный блок	HP PRO 3500	RUA31706ZG
2.	НЖМД	ST500DM002-1BD142	Z3TEDYW1
3.	Монитор	HP 2011x	CNC128RQ3K
4.	Клавиатура	HP PR1101U	BAUWF11RZ1I911
5.	Мышь	Genius NetScroll 100X	X75891203592
6.	Принтер	Ricoh SP 3510SF/Aficio SP 3510SF	T333Q201268
7.	Флешкарта	Smartbuy 4Gb	90005A612A3BF021
8.	Флешкарта	Kingmax PI-03G2 8Gb	3HAC0381400000352
9.	ИБП	APC Back-UPS CS 500	4B1137P05147

1.2 Аттестационная комиссия назначается генеральным директором АО «Гранит Информ», лицензия на деятельность по технической защите конфиденциальной информации № 0692 от 4 июля 2008 г.:

Рыжов К.С.– заместитель генерального директора АО «Гранит Информ», председатель комиссии;

Жаворонкин А.С. – ответственный за проведение аттестационных испытаний на соответствие организационно-техническим требованиям по защите информации, главный инженер АО «Гранит Информ», член комиссии;

Морар А.Ф. − ответственный за соответствие требованиям по защите информации от НСД, техник АО «Гранит Информ», член комиссии.

1.3 Целью аттестационных испытаний является проверка выполнения требований по безопасности информации на объекте информатизации согласно приказу ФСТЭК России № 21 от 18 февраля 2013 г. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Аттестация проводится на соответствие требованиям организационно-распорядительных и нормативных документов, перечень которых приведен в разделе 4.

1.4 Задачей аттестационных испытаний является оценка защищенности ИСПДн информации от утечки за счет:

– несанкционированного доступа к информации, обрабатываемой в ИСПДн;

– хищения технических средств, хранящейся в них информацией или отдельных носителей информации;

– просмотра информации с экранов дисплеев и других средств ее отображения с помощью оптических средств;

– воздействия на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, адресности и своевременности информационного обмена (электромагнитное, через специально внедренные программные средства («закладки»));

– несанкционированного перехвата информации, передаваемой по каналам связи.

1.5 При проведении аттестации применяются следующие методы проверок и испытаний:

– экспертно-документальный метод;

– проверка функций или комплекса функций защиты информации от НСД с помощью тестирующих средств, а также путем пробного запуска средств защиты информации от НСД и наблюдение за их выполнением;

1.5.1 Экспертно-документальный метод предусматривает проверку соответствия объекта информатизации установленным требованиям на основании экспертной оценки полноты и достаточности представленных документов по обеспечению необходимых мер защиты информации, а также соответствия реальных условий эксплуатации требованиям по размещению, монтажу и эксплуатации технических средств.

1.5.2 Проверка и испытания функций или комплекса функций защиты информации от НСД проводятся по выбору аттестационной комиссии для отдельных средств (технических и программных) ИСПДн или программно-технической среды в целом.

1.6 Испытания проводятся в эксплуатационных режимах работы объекта с использованием тестирующих программных средств. При отсутствии необходимых тестирующих средств они могут быть разработаны и использованы в процессе аттестационных испытаний. После окончания испытаний документация на дополнительно разработанные тестирующие средства прилагается к протоколам испытаний.

1.7 Объектом аттестационных испытаний является ИСПДн «Бухгалтерия» Общества с ограниченной ответственностью «Завод углеродных и композиционных материалов», уровня защищенности «4УЗ», класса защищенности от несанкционированного доступа к информации «1Г», размещенная по адресу: г. Челябинск, Челябинский электродный завод, 5 этаж, Бухгалтерия.

1.8 Перечень программных средств, с помощью которых проводится проверка выполнения требований по безопасности информации на объекте информатизации представлен в таблице 1.2.

Таблица 1.2 – **Перечень инструментальных средств**

Тип средства измерений	**Наименование**	**Заводской номер**	**Дата поверки**
Программа поиска и гарантированного уничтожения информации на дисках	«TERRIER» (версии 3.0)	Голограмма № А 293818	Сертификат ФСТЭК № 1193, действ. до 16.05.2018 г.
Программа фиксации и контроля исходного состояния программного комплекса	«ФИКС» (версия 2.0.1)	Голограмма № А 267757	Сертификат ФСТЭК № 913, действ. до 01.06.2019 г.
Средство создания модели системы разграничения доступа	«Ревизор 1 XP»	Голограмма № А 296220	Сертификат ФСТЭК № 989, действ. до 08.02.2020 г.
Программа контроля полномочий доступа к информационным ресурсам	«Ревизор 2 XP»	Голограмма № А 268720	Сертификат ФСТЭК № 990, действ. до 08.02.2020 г.

Тип средства измерений	Наименование	Заводской номер	Дата поверки
Программа поиска и контроля уязвимостей в вычислительных сетях	Сетевой сканер «Ревизор сети» версия 3.0	Голограмма № З 263216	Сертификат ФСТЭК № 3413 действителен до 02.06.2018 г.

1.9 Оценка соответствия объекта информатизации требованиям по безопасности информации производится на основании анализа общих результатов испытаний и выявленных в процессе испытаний недостатков и нарушений.

1.10 В случае выявления по результатам испытаний несоответствия ИСПДн установленным требованиям по защите информации комиссия может рассмотреть предложения заявителя по оперативному устранению выявленных недостатков и нарушений. При этом могут рекомендоваться следующие меры:

- доработка организационно-распорядительной документации;
- снижение уровня защищенности объекта информатизации;
- исключение отдельных средств из состава средств объекта информатизации;
- применение дополнительных организационно-технических мер защиты;
- применение дополнительных сертифицированных средств защиты информации.

1.11 Если в процессе аттестационных испытаний выявлены недостатки, не приводящие к нарушениям установленных требований и норм защищенности информации, то комиссия может рекомендовать следующие меры:

- оперативное устранение выявленных недостатков в процессе аттестационных испытаний;
- устранение установленных недостатков и нарушений, в согласованные с комиссией сроки, с представлением необходимых документов в АО «Гранит Информ»;
- проведение дополнительных испытаний по дополнительному соглашению;
- применение дополнительных организационно-технических мер защиты.

1.12 «Аттестат соответствия» выдается на основании вывода в Заключении по результатам аттестационных испытаний о возможности его выдачи.

2 ПРОГРАММА АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ

Аттестация проводится в соответствии с программой, включающей следующий перечень и порядок выполнения работ.

2.1 Предварительное ознакомление с составом, структурой и организацией эксплуатации объекта информатизации:

– анализ документов, определяющих состав и порядок эксплуатации;

– анализ размещения технических средств ИСПДн;

– проверка соответствия представленных заявителем исходных данных реальности, изучение технологического процесса обработки, передачи и хранения персональных данных, анализ информационных потоков.

2.2 Проверка правильности классификации объекта информатизации:

– проверка ПДн, циркулирующих в ИСПДн, для определения правильности категорирования ПДн;

– проверка уровня полномочий субъектов доступа к ИСПДн;

– проверка режимов обработки информации;

– проверка правильности определения уровня защищенности ИСПДн.

2.3 Проверка объекта информатизации на соответствие организационно-техническим требованиям по защите информации:

– проверка достаточности представленных документов и соответствия их содержания требованиям по безопасности информации;

– проверка уровня подготовки кадров и распределения ответственности персонала;

– проверка выполнения требований по безопасности информации к помещениям, в которых производится обработка информации.

2.4 Проведение испытаний объекта информатизации на соответствие требованиям по защите информации от НСД.

2.5 Проведение комплексных испытаний с целью оценки соответствия использованного комплекса мер и средств защиты требуемому уровню безопасности информации.

2.6 Подготовка отчетной документации и оценка результатов испытаний аттестуемого объекта.

2.6.1 Результаты аттестационных испытаний оформляются протоколом испытаний, содержащим:

– состав комиссии, дату испытаний, наименование аттестуемого объекта;

– цель испытаний;

– перечень нормативных документов и методик испытаний;

– результаты испытаний.

2.6.2 На основании полученных результатов испытаний принимается заключение, включающее:

– оценку соответствия объекта информатизации требованиям по безопасности информации;

– перечень выявленных недостатков и нарушений;

– рекомендации по устранению выявленных недостатков и нарушений;

– вывод о возможности (невозможности) выдачи «Аттестата соответствия».

3 МЕТОДИКА АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ПО БЕЗОПАСНОСТИ ИНФОРМАЦИИ

1.1. Общие положения.

Настоящая методика предназначена для проведения аттестационных испытаний ИСПДн «Бухгалтерия» Общества с ограниченной ответственностью «Завод углеродных и композиционных материалов», уровня защищенности «4УЗ», класса защищенности от несанкционированного доступа к информации «1Г», размещенная по адресу: г. Челябинск, Челябинский электродный завод, 5 этаж, Бухгалтерия на соответствие требованиям по безопасности информации.

Аттестационные испытания проводятся в следующем порядке:

– анализ полноты исходных данных, проверка их соответствия реальным условиям размещения, монтажа и эксплуатации;

– исследование технологического процесса обработки и хранения информации, анализ информационных потоков, определение состава использованных для обработки информации средств;

– проверка состояния организации работ и выполнения организационно – технических требований по защите информации, оценка правильности категорирования и классификации, оценка полноты разработки организационно – распорядительной, проектной и эксплуатационной документации, оценка уровня подготовки кадров и распределения ответственности за выполнение требований по обеспечению безопасности информации;

– проверка ИСПДн на соответствие требованиям по защите информации от НСД;

– подготовка отчетной документации.

1.2. Проведение испытаний.

1.2.1. Анализ полноты исходных данных, проверка их соответствия реальным условиям размещения, монтажа и эксплуатации технических средств ИСПДн.

Для проведения испытаний заявитель представляет аттестационной комиссии следующие исходные данные и документацию:

– технический паспорт на ИСПДн (в соответствии с приложением В СТР-К);

– акт присвоения уровня защищенности ИСПДн по требованиям защиты информации (в соответствии с Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»);

– сертификаты соответствия требованиям по безопасности информации на программные и технические средства ИСПДн, используемые средства защиты;

– состав технических и программных средств, входящих в ИСПДн;

– планы размещения ОТСС и ВТСС;

– план контролируемой зоны;

– схемы прокладки линий передачи данных ОТСС и ВТСС;

– состав и схемы размещения средств защиты информации;

– перечень ПДн;

– организационно-распорядительную документацию разрешительной системы доступа персонала к защищаемым ресурсам ИСПДн;

– описание технологического процесса обработки информации;

– частную модель угроз и требования к системе защиты;

– технологические инструкции пользователям ИСПДн;

– инструкции по эксплуатации средств защиты информации;

– документы, регламентирующие порядок и правила антивирусной защиты, восстановления конфиденциальной информации.

Приведенный перечень исходных данных и документации может уточняться по результатам анализа и проверки, в зависимости от особенностей объекта информатизации, по согласованию с аттестационной комиссией.

1.2.2. Исследование технологического процесса обработки и хранения информации, анализ информационных потоков, определение состава использованных для обработки информации технических средств.

1.2.2.1. При исследовании технологического процесса автоматизированной обработки и хранения информации исследуются следующие компоненты ИСПДн:

- объект доступа – средства обработки и передачи информации, информационные носители на магнитной и бумажной основе, накопители и все виды памяти ЭВМ, которые могут содержать информацию, отдельные документы и их архивы, используемые в технологическом процессе обработки информации, файлы, записи и другие информационные ресурсы, доступ к которым необходимо регламентировать;
- субъект доступа – персонал и все лица, которые имеют возможность доступа к средствам обработки информации, а также программные средства, посредством которых осуществляется доступ к объектам.

1.2.2.2. Используя исходные данные по технологии обработки и передачи информации, о разрешительной системе доступа персонала к защищаемым ресурсам, анализируется обобщенная технологическая схема ИСПДн с существующими и возможными информационными потоками, возможностями доступа к обрабатываемой и передаваемой информации.

1.2.2.3. Проверяется соответствие описания технологического процесса обработки, хранения и передачи ПДн реальному технологическому процессу обработки.

1.2.2.4. Проверяются паспортные (исходные) данные ИСПДн, комплектность и характеристики средств защиты и устанавливаются опасные факторы и угрозы, критические места ИСПДн, снижающие уровень защиты.

1.2.2.5. Проверяется наличие оформленных разрешений на допуск персонала к информации, соответствие технологических инструкций пользователей и администратора ИСПДн установленным требованиям по безопасности информации.

1.2.2.6. По результатам исследований уточняется схема технологического процесса в отношении отдельных средств обработки и передачи информации и штатного персонала.

1.2.3. Проверка состояния организации работ и выполнения организационно-технических требований по защите информации.

Проверка ИСПДн на соответствие организационно-техническим требованиям по защите информации проводится в объеме, указанном в таблице 3.1.

Таблица 3.1 – **Объем рабо**т

Наименование проверок и испытаний	**Пункт методики аттестационных испытаний**
Проверка достаточности представленных документов и соответствия их содержания требованиям по безопасности информации	3.2.3.1
Исследование технологического процесса обработки и хранения информации, анализ информационных потоков, определение состава использованных для обработки информации технических средств.	3.2.3.2
Проверка правильности категорирования КИ и классификации ИС	3.2.3.3
Проверка уровня подготовки кадров и распределения ответственности персонала	3.2.3.4

Наименование проверок и испытаний	Пункт методики аттестационных испытаний
Проверка наличия сертификатов соответствия на технические средства и средства защиты информации, экспертиза отчетов и протоколов по специальным исследованиям технических средств, предписаний на эксплуатацию технических средств	3.2.3.5
Проверка выполнения требований к помещениям, в которых производится обработка информации	3.2.3.6

1.2.3.1. Производится проверка достаточности представленных документов и соответствия их содержания требованиям стандартов и иным руководящим документам по безопасности информации ФСТЭК (Гостехкомиссии) России и других органов государственного управления в пределах компетенции.

1.2.3.2. С представленной документацией сверяется состав и структура программно-технических средств, включенных в реальный технологический процесс обработки информации. Определяются объекты и субъекты доступа, информационные потоки. Проверяется соответствие описания технологического процесса обработки и хранения защищаемой информации с реальной технологией обработки данных на объекте. Производится анализ вероятных опасных факторов и угроз, которые могут воздействовать на автоматизированную систему, а также возможных критических мест автоматизированной системы, снижающих уровень защиты. Анализируются средства и системы защиты информации, устраняющие выявленные опасные факторы и угрозы.

1.2.3.3. Проверка правильности присвоения уровня защищенности ИСПДн производится в соответствии с требованиями постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Проверка правильности классификации АС производится в соответствии с требованиями РД Гостехкомиссии России «Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации». Полученный уровень защищенности ИСПДн и класс АС сравнивается с установленным на объекте информатизации.

1.2.3.4. Проверка уровня подготовки кадров и распределения ответственности производится на основе следующих показателей:

- экспертной оценки знания инструкций по безопасности информации пользователями и эксплуатационным персоналом;
- наличия разрешительной системы доступа персонала к защищаемым ресурсам, определяющей полномочия по доступу к информации и процедуры их оформления, системы распределения ответственности персонала (оформленной приказами и распоряжениями начальника организации) за выполнение требований по безопасности информации;
- экспертной оценки системы технической учебы и повышения квалификации персонала и пользователей ИСПДн.

На основании опроса персонала проверяется знание исполнителями руководящих документов, необходимых технологических инструкций, предписаний, актов, заключений. Также проверяется уровень овладения персоналом технологией безопасной обработки информации, описанной в этих инструкциях.

1.2.3.5. Производится проверка наличия документов (сертификатов соответствия), подтверждающих возможность применения технических и программных средств, средств защиты процесса обработки информации. Производится экспертиза на соответствие требованиям нормативных документов протоколов по специальным исследованиям технических средств и предписаний на эксплуатацию технических средств.

1.2.3.6. Производится проверка выполнения требований руководящих документов по условиям размещения технических средств в помещениях, которые исключали бы возможность несанкционированного просмотра информации с экранов мониторов, с распечаток принтеров и с других устройств ввода-вывода информации.

1.2.3.7. По результатам проверки комиссия делает выводы о соответствии (или несоответствии) предъявленных документов и исходных данных установленным требованиям по безопасности информации.

1.2.4. Проверка ИСПДн на соответствие требованиям по защите информации

1.2.4.1. Анализ и оценка технологического процесса обработки информации

Комиссии представляется описание технологического процесса обработки информации на объекте информатизации, включающее в себя следующую информацию:

- перечень объектов доступа;
- перечень субъектов доступа;
- перечень штатных средств доступа к информации;
- перечень средств защиты информации;
- описание реализованных правил разграничения доступа;
- описание информационных потоков.

В качестве объектов доступа, в зависимости от класса АС, могут быть приняты:

- система в целом;
- терминалы, ЭВМ, узлы сети ЭВМ, каналы связи, внешние устройства ЭВМ;
- программы;
- тома, каталоги, файлы, записи, поля записей;
- все виды памяти ЭВМ, в которых может находиться информация.

В качестве субъектов доступа рассматриваются лица и процессы (программы пользователей), имеющие возможность доступа к объектам штатными средствами АС.

Под штатными средствами доступа к информации на АС понимаются общесистемные и прикладные средства и программы, предоставляющие субъектам документированные возможности доступа к объектам доступа.

Комиссия проверяет соответствие описания технологического процесса обработки и хранения конфиденциальной информации реальному процессу.

Проводится анализ разрешенных и запрещенных связей между субъектами и объектами доступа в отношении к отдельным средствам АС и штатному персоналу, оценка их соответствия разрешительной системе доступа персонала к защищаемым ресурсам на всех этапах обработки информации.

Проводится оценка опасных факторов и угроз, критических мест АС, снижающих уровень защиты; проверка наличия документов по разрешительной системе доступа персонала к защищаемой информации, хранящейся и (или) обрабатываемой в АС;

Проверка соответствия технологических инструкций пользователя и администратора защиты информации установленным требованиям.

1.2.4.2. Выбор средств и порядок испытаний на соответствие требованиям защиты информации от НСД уточняется на основании результатов анализа технологического процесса обработки информации.

1.2.4.3. Проверка подсистемы идентификации и аутентификации субъектов доступа и объектов доступа.

1.2.4.4. Проверка настройки управления доступом субъектов доступа к объектам доступа.

1.2.4.5. Проверка регистрации событий безопасности.

1.2.4.6. Проверка реализации антивирусной защиты.

1.2.4.7. Проверка наличия средства обнаружения вторжений и наличие обновлений баз решающих сигнатур.

1.2.4.8. Проверка реализации контроля защищенности персональных данных.

- Выявление уязвимостей информационной системы и оперативное устранение.
- Проверка установки обновлений ПО и программных средств СЗИ.
- Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и СЗИ.
- Контроль состава технических средств, ПО и СЗИ.
- Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализация правил разграничения доступа, полномочий пользователя в информационной системе.

1.2.4.9. Реализация требования по обеспечению целостности информационной системы и персональных данных.

- Целостность программных средств системы защиты информации обеспечивается проверкой контрольных сумм компонентов системы защиты при загрузке системы.
- Целостность программной среды обеспечивается отсутствием средств модификации объектного кода программ на рабочих станциях ИСПДн.

1.2.4.10. Защита технических средств.

- Проверка наличия пропускного режима.
- Проверка доступа посторонних лиц только при предъявлении документа, удостоверяющего личность. Защита информационной системы, ее средств, систем связи и передачи данных
- Проверка использования СЗИ, исключающих раскрытие, модификацию и навязывание информации при ее передаче по каналам связи, имеющим выход за пределы КЗ.

1.2.4.11. Реализация Защиты информационной системы, ее средств, систем связи и передачи данных.

1.2.4.12. Реализация выявления инцидентов, которые могут привести к сбоям или нарушению функционирования информационной системы и к возникновению угроз безопасности персональных данных, и реагирование на них.

- Проверка наличия лиц, ответственных за наличие инцидентов и реагирования на них.
- Проверка обнаружения, идентификации и регистрации инцидентов.
- Проверка принятия мер по устранению инцидентов.

1.2.4.13. Реализация управления конфигурацией информационной системы и системы защиты персональных данных.

- Проверка лиц, которые могут вносить изменения в конфигурацию информационной системы и СЗИ.
- Проверка изменений конфигураций информационной системы и системы защиты персональных данных.
- Анализ воздействия планируемых изменений.
- Проверка документов, регистрирующих изменение в конфигурации информационной системы и системы защиты персональных данных.

1.2.4.14. Испытания подсистемы антивирусной защиты.

Испытания антивирусной защиты заключаются в проверке наличия установленных лицензионных копий антивирусного обеспечения, проверке реализованных функций защиты от вредоносных программ и программно-математических воздействий, проверке соответствия антивирусной подсистемы требованиям РД к антивирусным системам в ИСПДн соответствующего класса. Также проверяется наличие необходимых инструкций на использование антивирусных средств.

4 ПЕРЕЧЕНЬ ОРГАНИЗАЦИОННО-РАСПОРЯДИТЕЛЬНЫХ И НОРМАТИВНЫХ ДОКУМЕНТОВ, НА СООТВЕТСТВИЕ КОТОРЫМ ПРОВОДЯТСЯ АТТЕСТАЦИОННЫЕ ИСПЫТАНИЯ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

4.1 Федеральный закон Российской Федерации от 27 июля 2006 г. 152-ФЗ «О персональных данных».

4.2 «Постановление об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1 ноября 2012 г. № 1119.

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

4.4 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».

4.5 «Методика определения актуальных угроз персональных данных при их обработке в информационных системах персональных данных» (Утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г.).

4.6 Руководящий документ «Защита от несанкционированного доступа к информации Термины и определения» (Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г.)

4.7 Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» (Утверждена решением Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.)

4.8 Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.)

4.9 Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.)

4.10 Руководящий документ «Защита от несанкционированного доступа к информации Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. № 114)

4.11 ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» введен в действие 01.01.1992 г.

4.12 ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем» введен в действие 01.01.1990 г.

4.13 ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадия создания»

4.14 ГОСТ 34.603-92 «Виды испытаний автоматизированных систем» введен в действие 01.01.1993 г.

4.15 ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования» введен в действие 01.01.1996 г.

4.16 ГОСТ Р 50922-96 «Защита информации. Основные термины и определения» введен в действие 01.07.1997 г.

4.17 ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» введен в действие 01.02.2008 г.

Руководитель аттестационной комиссии К.С. Рыжов

«_____»_____ 2018 г.

ПРИЛОЖЕНИЕ В

СОГЛАСОВАНО

Исполнительный директор Общества с ограниченной ответственностью «Завод углеродных и композиционных материалов»

_____ С.А. Подкопаев

«_____»_____ 2018 г.

УТВЕРЖДАЮ

Руководитель органа по аттестации объектов информатизации АО «Гранит Информ»

_____ Н.В. Узбеков

«_____»_____ 2018 г.

Общество с ограниченной ответственностью
«Завод углеродных и композиционных материалов»
г. Челябинск, Челябинский электродный завод, 5 этаж, Бухгалтерия

АКТ

обследования информационной системы персональных данных

«Бухгалтерия»

2018

В рамках аттестационных мероприятий сотрудниками АО «Гранит Информ» было проведено обследование информационной системы «Бухгалетрия» «Общества с ограниченной ответственностью «Завод углеродных и композиционных материалов» (далее ИСПДн), обрабатывающей персональные данные (далее ПДн).

Обследование проводилось путем:

– определения перечня ПДн, подлежащих защите;

– определения условий расположения ИСПДн относительно границ контролируемой зоны;

– определения конфигурации и топологии ИСПДн в целом и ее отдельных компонент, физических, функциональных и технологических связей как внутри ИСПДн, так и с другими системами различного уровня и назначения;

– определения режимов обработки информации в ИСПДн в целом и в ее отдельных компонентах;

– определения степени участия персонала в обработке ПДн, характер его взаимодействия между собой;

– определения уровня защищенности ИСПДн.

Предпроектное обследование проводилось путем:

– устного опроса лиц, ответственных за обработку ПДн;

– сбора информации о рабочих станциях, входящих в информационную систему, с использованием специального программного обеспечения;

– заполнения форм сбора информации об ИСПДн

1 ОБЩИЕ СВЕДЕНИЯ ОБ УЧРЕЖДЕНИИ

1.1 Реквизиты учреждения:

– полное наименование – Общество с ограниченной ответственностью «Завод углеродных и композиционных материалов»;

– адрес учреждения: г. Челябинск, Челябинский электродный завод.

1.2 ФИО и должность руководителя учреждения: Подкопаев С.А., Исполнительный директор Общества с ограниченной ответственностью «Завод углеродных и композиционных материалов».

1.3 Ответственный за обеспечение безопасности персональных данных: Кутов А.В., Заместитель исполнительного директора по персоналу и режиму.

1.4 Администратор безопасности на ОИ: Омельченко А.М., Руководитель направления обеспечения безопасности – специалист по защите информации.

2 СВЕДЕНИЯ ОБ ИСПДн

2.1 Территориальное размещение ИСПДн: локальная ИСПДн в пределах одного здания

2.2 Категория обрабатываемых ПДн: «Иные» т.к. в ИСПДн обрабатываются персональные данные субъектов персональных данных, не относящихся к категории специальных, биометрических и общедоступных.

2.3 Принадлежность обрабатываемых ПДн: сотрудников.

2.4 Тип актуальных угроз: для данной ИСПДн актуальны угрозы 3-го типа - не связаны с наличием недекларированных возможностей в программном обеспечении, используемом в ИСПДн.

2.5 Объем обрабатываемых ПДн: менее 100000.

2.6 Перечень ПДн:

– перечень персональных данных, указанных в Трудовом кодексе РФ.

2.7 Структура информационной системы: локальная информационная система.

2.8 Наличие соединения с сетями общего пользования и международного информационного обмена (МИО): ИСПДн имеет соединение с сетями общего пользования.

2.9 Режим обработки персональных данных: многопользовательский, с различными правами доступа.

2.10 Занимаемые помещения: Коммерческий отдел.

2.11 Количество пользователей ИСПДн: 1.

2.12 Информационное взаимодействие: данные заносятся с бумажных носителей.

2.13 Программное обеспечение, используемое для обработки персональных данных:

Таблица 1 – **Перечень ПО**

№	Наименование ПО	Версия
1	7-Zip	9.20.00.0
2	ABBYY FineReader 12 Corporate	12.1.609
3	Adobe Acrobat Reader DC	15.023.20053
4	Microsoft Office Professional Plus 2016	16.0.4266.1001
5	КОМПАС-3D Viewer	16.1
6	КриптоПро CSP	3.6.7777

2.14 Хранение персональных данных:

Хранение персональных данных осуществляется на ПК.

2.15 Используемые средства защиты информации на ОИ:

Таблица 2 – **Перечень СЗИ**

№	Наименование и тип средства защиты информации	Заводской номер	Сведения о сертификате	Место установки
1	СЗИ от НСД «Secret Net 7»	GL83EB81, Л 643287	№ 2707 от 07.09.2012 г.	В ПЭВМ
2	МЭ «Программный комплекс С-Терра Клиент Версия 4.1»	106096, К 169207	№ 3371 от 27.03.2015 г. № СФ/515-2659 от 20.07.2015 г.	В ПЭВМ
3	СКЗИ «Программный комплекс С-Терра Клиент Версия 4.1»	106096, К 169207	№ 3371 от 27.03.2015 г. СФ/114-2513 от 01.12.2017 г.	В ПЭВМ
4	САВЗ «Kaspersky Endpoint Security 10 для Windows»	СМП8069-8854, Л 874356	№ 3025 от 25.11.2013 г.	В ПЭВМ

2.16 Информация о физической охране ИСПДн: имеется физическая охрана, пропускной режим, видеонаблюдение.

2.17 Существующие документы, регламентирующие безопасность персональных данных:

– Положение по защите ПДн;

Комиссия в составе:

Председатель комиссии _____ К.С. Рыжов

Члены комиссии _____ А.С. Жаворонкин

_____ А.Ф. Морар

ПРИЛОЖЕНИЕ Г

УТВЕРЖДАЮ

Исполнительный директор Общества с ограниченной ответственностью «Завод углеродных и композиционных материалов»

_____ С.А. Подкопаев

«____» _____ 2018 г.

Акт
присвоения уровня защищенности
информационной системы персональных данных
«Бухгалетрия»
Общества с ограниченной ответственностью «Завод углеродных и композиционных материалов»

Комиссия в составе: председатель – Заместитель исполнительного директора по персоналу и режиму Кутов А.В., члены комиссии – Руководитель направления обеспечения безопасности – специалист по защите информации Омельченко А.М., Начальник режимно-секретного отдела Югатов Г.П., Начальник отдела информационных технологий Анферов А.В., назначенная Исполнительным директором Общества с ограниченной ответственностью «Завод углеродных и композиционных материалов», провела работу по определению и присвоению уровня защищенности ИСПДн «Бухгалтерия», расположенной по адресу: г. Челябинск, Челябинский электродный завод, Бухгалтерия.

Рассмотрев исходные данные об информационной системе персональных данных, определила:

1) категория персональных данных: «Иные» т.к. в ИСПДн обрабатываются персональные данные субъектов персональных данных, не относящихся к категории специальных, биометрических и общедоступных;

2) количество субъектов персональных данных: менее 100000;

3) актуальные угрозы безопасности персональных данных, являются угрозами 3 типа;

4) наличие взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена: ИСПДн физически отделенная от сети;

В соответствии с Постановлением «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», утвержденного Постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119 и на основании анализа исходных данных, РЕШИЛА:

информационной системе персональных данных «Бухгалтерия» Общества с ограниченной ответственностью «Завод углеродных и композиционных материалов» присвоить уровень защищенности: четвертый (**УЗ 4**).

Комиссия в составе:

Председатель комиссии _____ А.В. Кутов

Члены комиссии _____ А.М. Омельченко
_____ Г.П. Югатов
_____ А.В. Анферов

ПРИЛОЖЕНИЕ Д

УТВЕРЖДАЮ
Исполнительный директор
Общества с ограниченной ответственностью
«Завод углеродных и композитных
материалов»

_____С.А.Подкопаев
«___»_____г.Челябинск

Общество с ограниченной ответственностью «Завод углеродных и композитных материалов»
г. Челябинск, Челябинский электродный завод

МАТРИЦА ДОСТУПА
пользователей к защищаемым информационным ресурсам
информационной системы персональных данных
«Бухгалтерия»

г. Челябинск

Наименование информационных ресурсов, используемых в автоматизированной системе (логические диски, каталоги, программы, устройства и т.п.)	Тип доступа	Пользователи			
		Зуева Г.Ю. (Admin)	Зуева Г.Ю. (User1)	Горшкова С.А. (User2)	Витюк А.И. (User3)
1. Записи базы данных и электронные документы, в которых хранится информация ограниченного доступа	Чтение	Да	Да	Да	Да
	Добавление	Да	Да	Да	Да
	Модификация	Да	Да	Да	Да
	Удаление	Да	Да	Да	Да
2. НЖМД ID модели ST500DM002-1BD142 Серийный номер Z3TEDYW1	Чтение	Да	Да	Да	Да
	Запись	Да	Да	Да	Да
	Выполнение	Да	Да	Да	Да
3.Оптические диски	Чтение	Да	Да	Да	Да
	Запись	Да	Да	Да	Да
	Выполнение	Да	Нет	Нет	Нет
4. Флеш-карта Smartbuy 4Gb Серийный номер 90005A612A3BF021	Чтение	Да	Да	Да	Да
	Запись	Да	Да	Да	Да
	Выполнение	Да	Нет	Нет	Нет
5. Флеш-карта Kingmax PI-03G2 8Gb Серийный номер 3HAC0381400000352	Чтение	Да	Да	Да	Да
	Запись	Да	Да	Да	Да
	Выполнение	Да	Нет	Нет	Нет
6. Принтер Ricoh SP 3510SF/Aficio SP 3510SF Серийный номер T333Q201268	Печать	Да	Да	Да	Да
7. C:\ПДн	Чтение	Да	Да	Да	Да
	Добавление	Да	Да	Да	Да
	Модификация	Да	Да	Да	Да
	Удаление	Да	Да	Да	Да
8. Системные политики	Настройка	Да	Нет	Нет	Нет
9. Программные средства	Настройка	Да	Нет	Нет	Нет
	Выполнение	Да	Да	Да	Да
10. Средства защиты информации	Настройка	Да	Нет	Нет	Нет
11. Антивирус	Настройка	Да	Нет	Нет	Нет
	Обновление	Да	Нет	Нет	Нет
12. Доступ к внешним сетям	Доступ к ресурсам локальной сети организации	Да	Да	Да	Да

Наименование информационных ресурсов, используемых в автоматизированной системе (логические диски, каталоги, программы, устройства и т.п.)	Тип доступа	Пользователи			
		Зуева Г.Ю. (Admin)	Зуева Г.Ю. (User1)	Горшкова С.А. (User2)	Витюк А.И. (User3)
	Доступ к сетям связи общего пользования	Да	Да	Да	Да

Ответственный по защите информации на объекте информатизации, Заместитель исполнительного директора по персоналу и режиму _____ Кутов А.В.

ПРИЛОЖЕНИЕ Е

УТВЕРЖДАЮ
Исполнительный директор
Общества с ограниченной ответственностью
«Завод углеродных и композитных
материалов»

_____С.А.Подкопаев
«____» _____ 2018 г.

ОПИСАНИЕ
ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА ОБРАБОТКИ ИНФОРМАЦИИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ
«Бухгалтерия»
Общества с ограниченной ответственностью
«Завод углеродных и композиционных материалов»

2018 г.

1 ОБЩИЕ ПОЛОЖЕНИЯ

Настоящий документ регламентирует технологию автоматизированной обработки информации в информационной системе персональных данных «АРМ 2» (далее ИСПДн) Общества с ограниченной ответственностью «Завод углеродных и композиционных материалов», по адресу: г. Челябинск, Челябинский электродный завод, Бухгалтерия.

Настоящий документ разработан с целью определения и описания основных технических и программных средств обработки персональных данных, объектов и субъектов доступа, функциональных связей между ними, средств ввода, вывода, передачи информации, используемых средств защиты информации и общей технологии автоматизированной обработки персональных данных в системе.

2 СОСТАВ ИСПДн

Состав основных технических средств и систем (ОТСС) и ИСПДн приведен в таблице

Таблица 1 - Состав ОТСС ИСПДн

№ п/п	Наименование устройства	Фирма производитель, Модель	Заводской/ инвентаризационный номер
1.	Системный блок	HP PRO 3500	RUA31706ZG
2.	НЖМД	ST500DM002-1BD142	Z3TEDYW1
3.	Монитор	HP 2011x	CNC128RQ3K
4.	Клавиатура	HP PR1101U	BAUWF11RZ1I911
5.	Мышь	Genius NetScroll 100X	X75891203592
6.	Принтер	Ricoh SP 3510SF/Aficio SP 3510SF	T333Q201268
7.	Флешкарта	Smartbuy 4Gb	90005A612A3BF021
8.	Флешкарта	Kingmax PI-03G2 8Gb	3HAC0381400000352
9.	ИБП	APC Back-UPS CS 500	4B1137P05147

3 ОБЪЕКТЫ ДОСТУПА

Объектами доступа в ИСПДн являются:

– ОТСС, предназначенные для обработки и передачи ПДн;

– программные средства ИСПДн, предназначенные для обработки и передачи ПДн;

– учтенные машинные носители информации (далее - МНИ): компакт-диски, несъемные НЖМД, съемные флэш-накопители;

– все виды памяти ПЭВМ ИСПДн, в которой может находиться защищаемая информация.

4 СУБЪЕКТЫ ДОСТУПА

Субъектами доступа в ИСПДн являются:

– пользователи, допущенные к работам в ИСПДн на основании приказа руководителя;

– штатные программные средства пользователей ИСПДн.

5 СРЕДСТВА ОБРАБОТКИ И ПЕРЕМЕЩЕНИЯ ИНФОРМАЦИИ

Средствами обработки и перемещения информации в ИСПДн являются:

– Штатные программные средства ИСПДн, предоставляющие субъектам документированные возможности доступа к объектам доступа.

– Штатные технические средства ИСПДн, предоставляющие субъектам документированные возможности доступа к объектам доступа.

6 ПЕРЕЧЕНЬ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Перечень средств защиты информации, используемых в ИСПДн приведен в таблице 2.

Таблица 2 - Перечень СЗИ

№	Наименование средств защиты	Заводской номер, СЗЗ	Сведения о сертификате
1.	СЗИ от НСД «Secret Net 7»	GL83EB81, Л 643287	№ 2707 от 07.09.2012 г.
2.	МЭ «Программный комплекс С-Терра Клиент Версия 4.1»	106096, К 169207	№ 3371 от 27.03.2015 г. № СФ/515-2659 от 20.07.2015 г.
3.	СКЗИ «Программный комплекс С-Терра Клиент Версия 4.1»	106096, К 169207	№ 3371 от 27.03.2015 г. СФ/114-3227 от 01.12.2017 г.
4.	САВЗ «Kaspersky Endpoint Security 10 для Windows»	СМП8069-8854, Л 874356	№ 3025 от 25.11.2013 г.

7 ОПИСАНИЕ РЕАЛИЗОВАННЫХ ПРАВИЛ РАЗГРАНИЧЕНИЯ ДОСТУПА

Пользователи допущены только к определенным защищаемым ресурсам с различными правами согласно разрешительной системе доступа.

8 ОБОБЩЕННАЯ СХЕМА АВТОМАТИЗИРОВАННОЙ ОБРАБОТКИ ИНФОРМАЦИИ В ИСПДн

8.1 Перед обработкой ПДн:

8.1.1 В случае необходимости, пользователь получает учтенные съемные носители.

8.1.2 Пользователь заходит в помещение ИСПДн. Производит контроль отсутствия в помещении посторонних лиц. Включает питание ПЭВМ.

8.1.3 По запросу СЗИ пользователь вводит свой идентификатор и текущий пароль или предъявляет персональный аппаратный ключ. После ввода правильных данных происходит вход в операционную систему.

8.1.4 Пользователь запускает программное обеспечение доступа к базе персональных данных. В случае необходимости, вводит свой идентификатор и пароль для доступа к базе данных. После ввода правильных данных происходит создание сеанса работы с базой данных.

8.2 При обработке ПДн:

8.2.1 В зависимости от выполняемых должностных обязанностей пользователь осуществляет чтение, модификацию, добавление или удаление персональных данных.

8.2.2 При необходимости пользователь осуществляет вывод на печать части ПДн. На печать могут выводиться приказы, справки, распоряжения, отчёты, содержащие персональные данные.

8.3 Особенности обработки ПДн:

8.3.1 Персональные данные в ИСПДн заносятся с бумажных и учтенных внешних машинных носителей.

8.4 По окончанию работы пользователь ИСПДн:

8.4.1 Пользователь завершает сеанс работы с базой персональных данных.

8.4.2 Пользователь завершает работу операционной системы и выключает питание ПЭВМ. При необходимости, закрывает помещение ИСПДн.

8.4.3 Сдаёт все учтённые съёмные носители информации.

8.5 В процессе эксплуатации объекта информатизации администратор безопасности:

– контролирует технологический процесс обработки ПДн в ИСПДн;

– выполняет администрирование СЗИ, назначает права пользователям ИСПДн в системе, создает и блокирует (удаляет) учетные записи пользователей ИСПДн;

– анализирует журналы регистрации СЗИ с целью обнаружения в них попыток НСД к защищаемой информации;

– контролирует процесс смены пользователями ИСПДн паролей доступа в систему в предписанные сроки;

– контролирует функционирование антивирусного программного обеспечения, обеспечивает периодическое обновление антивирусных баз, анализирует журналы их работы;

– консультирует пользователей ИСПДн по вопросам функционирования СЗИ, антивирусного программного обеспечения и по вопросам обеспечения защиты ПДн от НСД.

Ответственный за обеспечение
безопасности персональных данных,
Заместитель исполнительного
директора по персоналу и режиму _____ А.В. Кутов

Администратор безопасности,
Руководитель направления обеспечения
безопасности – специалист по защите информации _____ А.М. Омельченко

ПРИЛОЖЕНИЕ Ж

УТВЕРЖДАЮ
Исполнительный директор
Общества с ограниченной ответственностью
«Завод углеродных и композитных
материалов»

_____С.А.Подкопаев
«____» _____ 2018 г.

ПОЛОЖЕНИЕ
об обработке и защите персональных данных
Общества с ограниченной ответственностью «Завод углеродных и композитных материалов»

2018

1 Введение.

1.1. Настоящее Положение об обработке и защите персональных данных Общества с ограниченной ответственностью «Завод углеродных и композитных материалов» (далее Положение) определяет порядок обработки персональных данных сотрудников Общества с ограниченной ответственностью «Завод углеродных и композитных материалов», расположенной по адресу г. Челябинск, Челябинский электродный завод (далее – Организации).

1.2. Настоящее Положение разработано на основании и во исполнение Федерального закона РФ «О персональных данных» от 27.07.2006г. № 152-ФЗ (Далее –ФЗ 152) и других нормативных правовых актов Российской Федерации, регулирующих отношения, связанные с обработкой персональных данных.

1.3. Настоящее Положение разработано в целях определения порядка обработки персональных данных физических лиц, обеспечения конфиденциальности и безопасности персональных данных при их обработке, защиты конституционных прав и свобод граждан, в том числе на неприкосновенность частной жизни, личную и семейную тайну, при их обработке в Организации. Положение распространяет свое действие как на случаи обработки Организацией персональных данных собственных работников, так и на случае обработки Организацией персональных данных иных лиц.

1.4. Настоящее Положение является локальным нормативным актом Организации и подлежит обязательному исполнению всеми работниками Организации. Каждый работник Организации должен быть ознакомлен с требованиями настоящего Положения.

2. Термины и определения.

2.1. Для целей настоящего Положения используются следующие термины и определения:

- персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;
- 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;
- автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;
- распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
- предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
- блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
- уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

- обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
- информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

3. Принципы обработки ПДн.

3.1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

3.2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3.3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

3.4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

3.5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

3.6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

3.7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

3.8. Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных Федеральным законом.

4. Цели, основания и способы обработки ПДн.

4.1. Руководствуясь действующим законодательством РФ, другими нормативными правовыми актами, в пределах своих полномочий и задач, определенных Уставом, Организация самостоятельно определяет цели обработки ПДн, устанавливает правовые основания такой обработки.

4.2. Обработка персональных данных допускается в случаях, предусмотренных ФЗ «О персональных данных», в частности:

4.2.1. обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

4.2.2. обработка персональных данных необходима для достижения целей, предусмотренных законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

4.2.3. обработка персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

4.2.4. обработка персональных данных необходима для исполнения договора, стороной которого является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных;

4.2.5. обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

4.2.6. обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц;

4.2.7. обработка персональных данных осуществляется в статистических целях, при условии обязательного обезличивания персональных данных;

4.2.8. осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее - персональные данные, сделанные общедоступными субъектом персональных данных).

4.3. Установленные Организацией цели и правовые основания обработки ПДн утверждаются приказом Исполнительного директора Общества с ограниченной ответственностью «Завод углеродных и композитных материалов» Общества с ограниченной ответственностью «Завод углеродных и композитных материалов» в отношении каждой категории субъектов ПДн.

4.4. Организация обрабатывает ПДн следующими способами:

- на бумажных носителях;
- в ИСПДн с использованием и без использования средств вычислительной техники, а также смешанным способом;
- в ИСПДн без участия и при непосредственном участии человека.

4.5. Организация самостоятельно устанавливает способы обработки ПДн в зависимости от целей такой обработки и собственных материально-технических возможностей.

5. Категории ПДн и категории субъектов ПДн.

5.1. Организация осуществляет обработку следующих категорий ПДн: Иные

5.2. Организация осуществляет обработку следующих категорий субъектов ПДн: сотрудников

5.3. Категории ПДн и категории субъектов ПДн, подлежащих обработке, определяются Организацией на основании и во исполнение действующего законодательства РФ, других нормативных правовых актов.

6. Срок обработки ПДн.

6.1. Общий срок обработки ПДн определяется периодом времени, в течение которого Организация осуществляет в отношении ПДн предусмотренные законом и обусловленные заявленными целями их обработки действия (операции), в том числе хранение ПДн.

6.2. Течение срока обработки ПДн начинается с момента их получения Организацией и заканчивается (в случае, если иного не предусмотрено федеральным законом) уничтожением или обезличиванием ПДн:

- по достижении заранее заявленных целей обработки;
- по факту утраты необходимости в достижении заранее заявленных целей обработки.

6.3. Организация осуществляет хранение ПДн в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

6.4. Конкретные сроки обработки, в том числе сроки хранения ПДн, должны быть установлены Организацией в отношении каждого субъекта ПДн.

7. Условия обработки ПДн.

7.1. Обработка ПДн должна осуществляться с соблюдением принципов, предусмотренных ФЗ 152 и настоящим Положением.

7.2. Получение персональных данных осуществляется оператором лично у каждого субъекта персональных данных, либо у его представителя, имеющего соответствующие полномочия.

7.3. Персональные данные могут быть получены от лица, не являющегося субъектом персональных данных, при условии предоставления оператору подтверждения наличия оснований, указанных в подпунктах 4.2.2-4.2.8 настоящего Положения.

7.4. Обработка ПДн должна осуществляться с соблюдением следующих правил:

7.4.1. обработка ПДн возможна лишь при наличии конкретной определенной законной и обоснованной цели. Иная обработка ПДн не допускается;

7.4.2. обработка ПДн обоснована и допустима тогда, когда она осуществляется в случаях, которые прямо названы в ст.ст.6, 10, 11 ФЗ 152;

7.4.3. при обработке ПДн запрещается раскрывать третьим лицам и распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

7.4.4. обработка ПДн может быть поручена другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора и при условии, что такое поручение оператора содержит:

- перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных;
- цели обработки;
- обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке;
- требования к защите обрабатываемых персональных данных в соответствии со статьей 19 ФЗ 152.

7.5. В случае если для отдельных операций с ПДн или для отдельных случаев обработки ПДн законодательством предусмотрены дополнительные правила и требование, такая обработка должна осуществляться в соответствии с этими правилами и требованиями.

8. Уточнение, блокирование и уничтожение ПДн.

8.1. Уточнение ПДн, в том числе их обновление и изменение, имеет своей целью обеспечение точности персональных данных, их достаточности, а в необходимых случаях и актуальности по отношению к целям обработки персональных данных, обрабатываемых Организацией.

8.2. Организация осуществляет уточнение ПДн или обеспечивает их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) по собственной инициативе, при обращении субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных в случае, когда установлено, что ПДн являются неточными, неполными, устаревшими, недостоверными.

8.3. Блокирование ПДн имеет своей целью временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения персональных данных) до момента устранения обстоятельств, послуживших основанием для блокирования ПДн.

8.4. Организация осуществляет блокирование ПДн или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) при обращении субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного

органа по защите прав субъектов персональных данных в случае выявления неточных ПДн или неправомерной их обработки.

8.5. Организация прекращает обработку и уничтожает ПДн или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора):

- по достижении цели обработки ПДн;
- в случае утраты необходимости в достижении целей обработки ПДн;
- в случае отзыва субъектом ПДн согласия на обработку своих ПДн, если сохранение персональных данных более не требуется для целей обработки персональных данных;
- в случае если ПДн являются незаконно полученными;
- по требованию субъекта ПДн или уполномоченного органа по защите прав субъектов ПДн в случае выявления фактов совершения Организацией или лицом, действующим по поручению оператора, неправомерной обработки ПДн, если обеспечить правомерность обработки персональных данных невозможно.

8.6. В целях обеспечения законности при обработке ПДн и устранения факторов, влекущих или могущих повлечь неправомерные действия с ПДн, Организация вправе по собственной инициативе осуществить блокирование и уничтожение ПДн.

9. Способы обработки персональных данных

9.1. Оператор осуществляет неавтоматизированную и автоматизированную обработку персональных данных.

9.2. Неавтоматизированную и автоматизированную обработку персональных данных, включая доступ к соответствующим персональным данным, осуществляют работники оператора согласно перечню должностей, утвержденному Приказом директора предприятия.

9.3. Неавтоматизированная обработка персональных данных.

9.3.1. Обработка персональных данных, содержащихся в информационной системе либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

9.3.2. При неавтоматизированной обработке должны соблюдаться следующие требования:

9.3.2.1. Персональные данные при их обработке должны обособляться от иной информации, в частности путем фиксации на отдельных материальных носителях, в специальных разделах или на полях форм (бланков). Не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы.

9.3.2.2. Работники оператора должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, об особенностях и правилах такой обработки.

9.3.2.3. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;
- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных,

осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;

- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;
- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

9.3.3. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

- при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;
- при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

9.3.4. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

9.3.5. Вышеуказанные правила применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

9.3.6. Уточнение персональных данных производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

9.3.7. В отношении каждой категории персональных данных определяются места хранения персональных данных (материальных носителей), при этом хранение персональных данных, обработка которых осуществляется в различных целях, обеспечивается раздельно.

9.4. Автоматизированная обработка персональных данных.

9.4.1. При автоматизированной обработке должно быть обеспечено:

9.4.1.1. проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

9.4.1.2. своевременное обнаружение фактов несанкционированного доступа к персональным данным;

9.4.1.3. недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

9.4.1.4. возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

9.4.1.5. постоянный контроль за обеспечением уровня защищенности персональных данных.

9.4.2. Обеспечение безопасности персональных данных при их обработке в информационной системе осуществляется оператором в соответствии с организационно-распорядительными документами Организации.

10. Обязанности Организации при обращении либо при получении запроса субъекта ПДн (его представителя) или уполномоченного органа по защите прав субъектов ПДн.

10.1. Организация обязана в порядке и в сроки, предусмотренные действующим законодательством РФ, сообщить субъекту ПДн или его представителю информацию о наличии ПДн, относящихся к соответствующему субъекту ПДн, а также предоставить возможность ознакомления с ними при обращении субъекта ПДн или его представителя.

10.2. Организация обязана сообщить в уполномоченный орган по защите прав субъектов ПДн по его запросу информацию, необходимую для осуществления деятельности указанного органа.

10.3. В указанных в п.п. 9.1., 9.2. настоящего Положения целях Исполнительный директор Общества с ограниченной ответственностью «Завод углеродных и композитных материалов» совместно с руководителями структурных подразделений (отделов), непосредственно связанных с осуществлением деятельности по обработке ПДн, обеспечением защиты ПДн и организацией делопроизводства разрабатывает и утверждает Регламент действий при обращении либо при получении запроса субъекта ПДн (его представителя) или уполномоченного органа по защите прав субъектов ПДн.

11. Устранение нарушений законодательства, допущенных при обработке ПДн.

11.1. В случае выявления в деятельности Организации каких-либо нарушений законодательства, допущенных при обработке ПДн, Организация устраняет такие нарушения в порядке и сроки, установленные федеральными законами.

12. Меры по обеспечению безопасности ПДн при их обработке.

12.1. Организация при обработке ПДн принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие, для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении персональных данных.

12.2. В целях реализации п. 10.1. Организацией разрабатываются и утверждаются:

- планы мероприятий по защите ПДн;
- планы внутренних проверок состояния защищенности ПДн;
- списки лиц, доступ которых к ПДн, обрабатываемым в ИСПДн, необходим для выполнения служебных (трудовых) обязанностей;
- локальные нормативные акты и должностные инструкции;
- иные документы, регулирующие порядок обработки и обеспечения безопасности и конфиденциальности ПДн.

12.3. Обеспечение безопасности персональных данных Организации достигается, в частности:

- определением угроз безопасности ПДн при их обработке в ИСПДн Организации;
- применением организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн Организации, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивают установленные Правительством Российской Федерации уровни защищенности персональных данных;

- применением прошедших в установленном порядке процедуру оценки соответствия, а в случае необходимости - аттестацию средств защиты информации;
- оценкой эффективности принимаемых Организацией мер по обеспечению безопасности персональных данных до ввода в эксплуатацию ИСПДн Организации;
- учетом машинных носителей ПДн Организации;
- обнаружением фактов НСД к ПДн и принятием мер;
- восстановлением ПДн, которые были модифицированы или уничтожены вследствие НСД к ним;
- установлением правил доступа к ПДн, обрабатываемым в ИСПДн Организации, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в ИСПДн Организации;
- контролем за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн Организации.

12.4. Организация выполняет требования к защите персональных данных при их обработке в ИСПДн Организации, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности ПДн в зависимости от угроз безопасности этих данных с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных.

13. Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим Федеральным законом.

13.1. Организация принимает все необходимые и достаточные меры для обеспечения выполнения обязанностей, предусмотренных Федеральным законом и другими нормативными правовыми актами.

13.2. В целях реализации п. 11.1. Организации:

- назначает ответственного за организацию обработки персональных данных;
- применяет правовые, организационные и технические меры по обеспечению безопасности персональных данных в соответствии с требованиями закона;
- осуществляет внутренний контроль (аудит) соответствия обработки персональных данных ФЗ 152 и другим нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;
- оценивает вред, который может быть причинен субъектам персональных данных в случае нарушения ФЗ 152;
- знакомит своих работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, организует и (или) обеспечивает обучение указанных работников.

14. Ответственность за нарушения, допущенные при обработке ПДн.

14.1. Каждый работник Организации должен быть ознакомлен с содержанием настоящего Положения под роспись. Расписка об ознакомлении приобщается к личному делу работника.

14.2. Работники и должностные лица Организации, виновные в нарушении требований федерального законодательства и иных нормативных правовых актов, регулирующих отношения в сфере обработки ПДн и обеспечения их безопасности и конфиденциальности, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

14.3. Организация возмещает в соответствии с законодательством РФ вред, причиненный субъекту ПДн вследствие нарушения его прав, нарушения правил обработки персональных

данных, а также требований к защите персональных данных.

15. Заключительные положения.

15.1. Настоящее Положение вступает в силу с момента утверждения приказом Исполнительного директора Общества с ограниченной ответственностью «Завод углеродных и композитных материалов» и действует без ограничения срока.

15.2. Настоящее Положение не заменяет собой действующего законодательства РФ, регулирующего общественные отношения в сфере обработки ПДн и обеспечения их безопасности и конфиденциальности.

15.3. Настоящее Положение подлежит корректировке при изменении законодательных и нормативно-правовых актов, по рекомендациям надзорных органов, по результатам проверок в рамках государственного контроля, а также в целях совершенствования технологий обработки ПДн.

15.4. Изменения к Положению утверждает Исполнительный директор Общества с ограниченной ответственностью «Завод углеродных и композитных материалов».

15.5. В случае если в результате изменений федеральных законов и иных нормативных правовых актов отдельные требования настоящего Положения вступят в противоречие с указанными законами и нормативными правовым актами, соответствующие требования Положение не будут подлежать применению.

С «Положением об обработке и защите персональных данных Общества с ограниченной ответственностью «Завод углеродных и композитных материалов»» ознакомлены:

Дата	**Ф.И.О.**	**Подпись**

ПРИЛОЖЕНИЕ З

СОГЛАСОВАНО

Руководитель органа по аттестации
объектов информатизации
АО «Гранит Информ»

_____ Н.В. Узбеков
«_____»_____ 2018 г.

УТВЕРЖДАЮ

Исполнительный директор Общества с
ограниченной ответственностью «Завод уг-
леродных и композиционных материалов»

_____ С.А. Подкопаев
«_____»_____ 2018 г.

Общество с ограниченной ответственностью
«Завод углеродных и композиционных материалов»
г. Челябинск, Челябинский электродный завод

ЧАСТНАЯ МОДЕЛЬ УГРОЗ
безопасности персональных данных
при их обработке в информационной системе персональных данных
«Бухгалтерия»

2018 г.

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Данная частная модель безопасности персональных данных при их обработке в информационной системе персональных данных «Бухгалтерия» Исполнительный директор Общества с ограниченной ответственностью «Завод углеродных и композиционных материалов» (далее – ИСПДн) разработана на основании:

– «Базовой модели угроз безопасности персональных данных при обработке в информационных системах персональных данных», утвержденной 15 февраля 2008 г. заместителем директора ФСТЭК России;

– «Методики определения актуальных угроз безопасности персональных данных при обработке в информационных системах персональных данных», утвержденной 14 февраля 2008 г. заместителем директора ФСТЭК России;

– ГОСТ Р 51275-2006 «Защита информации. Факторы, воздействующие на информацию. Общие положения».

1.2 Модель определяет угрозы безопасности персональных данных, обрабатываемых в информационной системе персональных данных «Бухгалтерия».

2 ПЕРЕЧЕНЬ УГРОЗ, ПРЕДСТАВЛЯЮЩИХ ПОТЕНЦИАЛЬНУЮ ОПАСНОСТЬ ДЛЯ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ИСПДн

Потенциальную опасность безопасности персональных данных (далее – ПДн) при их обработке в ИСПДн представляют:

– несанкционированный доступ к ПДн, обрабатываемым в ИСПДн;
– утечка информации по техническим каналам;
– несанкционированный доступ к рабочим станциям пользователей;
– несанкционированный доступ к серверам;
– утечка ПДн с использованием внешних носителей информации;
– утечка ПДн по сетям связи общего пользования.

3 ОПРЕДЕЛЕНИЕ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПДн ПРИ ОБРАБОТКЕ В ИСПДн

3.1 Определение уровня исходной защищенности ИСПДн.

Уровень исходной защищенности ИСПДн определен экспертным методом в соответствии с «Методикой определения актуальных угроз безопасности персональных данных при обработке в информационных системах персональных данных» (далее – Методика), утвержденной 14 февраля 2008 г. заместителем директора ФСТЭК России. Результаты анализа исходной защищенности приведены в таблице 2 Глава 2.6.

3.2 Определение актуальных угроз безопасности ПДн.

Определение опасности угроз безопасности ПДн проведено экспертным методом на основе опроса экспертов (специалистов в области защиты информации) с учётом результатов обследования ИСПДн. Определение актуальных угроз безопасности ПДн проведено экспертным методом в соответствии с «Методикой…». Результаты определения опасности угроз с мнениями экспертов и определения актуальных угроз безопасности приведены в таблице 1.

Таблица 1 – Определение актуальных угроз

Наименование угрозы	Y_2	Y	Возможность реализации угрозы	Опасность угрозы	Меры по противодействию угрозе		Актуальность угрозы
					Технические	Организационные	
I Угрозы утечки по техническим каналам							
1.1 Угрозы утечки акустической информации							
1.1.1 Непреднамеренное разглашение информации сотрудниками лицам, не допущенным к обработке персональных данных	2	0,35	Средняя	Низкая	Дверь в помещение с ИСПДн оборудована замком	Инструкция пользователя, Технологический процесс	Неактуальная
1.1.2 Снятие виброакустического сигнала со строительных конструкций и инженерно-технических коммуникаций помещений	0	0,25	Низкая	Низкая	В ИСПДн не обрабатываются информация ограниченного доступа с использованием акустического канала.		Неактуальная
1.1.3 Акустоэлектрические и акустооптические преобразования	0	0,25	Низкая	Низкая			Неактуальная
1.2 Угрозы утечки видовой информации							
1.2.1 Просмотр информации на дисплее сотрудниками, не допущенными к обработке персональных данных	0	0,25	Низкая	Низкая	Дверь в помещение оборудована замком, помещение оснащено охранной сигнализацией. СЗИ от НСД «Secret Net 7»	Документы: Инструкция пользователя, Мероприятия: Расположение экрана монитора, исключающее просмотр содержимого другими лицами; пропускной режим	Неактуальная
1.2.2 Просмотр информации на дисплее посторонними лицами, находящимися в помещении, в котором ведется обработка персональных данных	0	0,25	Низкая	Низкая	Дверь в помещение с ИСПДн оборудована замком, помещение оснащено охранной сигнализацией. Установлено СЗИ от НСД «Secret Net 7»	Документы: Инструкция пользователя, Мероприятия: Расположение экрана монитора, исключающее просмотр содержимого другими лицами; пропускной режим	Неактуальная
1.2.3 Просмотр информации на дисплее посторонними лицами, находящимися за пределами помещения, в котором ведется обработка персональных данных	0	0,25	Низкая	Низкая	Жалюзи на окно	Документы: Инструкция пользователя, Мероприятия: Расположение экрана монитора, исключающее просмотр содержимого другими лицами	Неактуальная
1.2.4 Просмотр информации с помощью специальных электронных устройств внедренных в помещении, в котором ведется обработка персональных данных	0	0,25	Низкая	Низкая	Дверь в помещение с ИСПДн оборудована замком, помещение оснащено охранной сигнализацией	Порядок пропускного режима	Неактуальная
1.3 Угрозы утечки информации по каналам ПЭМИН							
1.3.1 Угрозы преднамеренного электромагнитного воздействия на элементы ИСПДн	0	0,25	Низкая	Низкая	Руководством ООО «Завод углеродных и композиционных материалов» канал ПЭМИН признан неактуальным.		Неактуальная
1.3.2 Утечка информации по сетям электропитания	0	0,25	Средняя	Низкая			Неактуальная
1.3.3 Утечка за счет наводок на линии связи, технические средства, расположенные в помещении, и системы коммуникаций	0	0,25	Низкая	Низкая			Неактуальная

Продолжение Таблицы 1

Наименование угрозы	Y_2	Y	Возможность реализации угрозы	Опасность угрозы	Меры по противодействию угрозе		Актуальность угрозы
					Технические	Организационные	
1.3.4 Побочные излучения технических средств	0	0,25	Низкая	Низкая			Неактуальная
I Угрозы несанкционированного доступа к информации							
2.1 Угрозы уничтожения, хищения аппаратных средств ИСПДн, носителей информации, информации путем физического доступа							
2.1.1 Кража ПЭВМ	0	0,25	Низкая	Средняя	Дверь в помещение с ИСПДн оборудована замком, помещение оснащено охранной сигнализацией	Пропускной режим, Охрана, Акт установки средств защиты, Инструкция пользователя, Приказ об определении границ контролируемой зоны, Учет носителей информации	Неактуальная
2.1.2 Кража носителей информации	0	0,25	Низкая	Средняя	Дверь в помещение с ИСПДн оборудована замком, охранная сигнализация, хранение в сейфе		Неактуальная
2.1.3 Кража ключей доступа	0	0,25	Низкая	Средняя	Дверь в помещение оборудована замком, помещение оснащено охранной сигнализацией, хранение в сейфе	Инструкция пользователя, Инструкция администратора безопасности, Инструкция парольной защиты, Матрица доступа пользователей	Неактуальная
2.1.4 Кража, модификация, уничтожение информации.	0	0,25	Низкая	Средняя	Установлено средство защиты от НСД «Secret Net 7»		Неактуальная
2.1.5 Вывод из строя узлов ПЭВМ, каналов связи	0	0,25	Низкая	Низкая	Дверь в помещение с ИСПДн оборудована замком, помещение оснащено охранной сигнализацией	Документы: Инструкция пользователя, Технологический процесс, Список лиц допущенных к обработке, Разрешительная система доступа, Положение о защите ПДн, Инструкция администратора, Технический паспорт, Журнал учета машинных носителей, Соглашение о неразглашении. Мероприятия: Своевременная замена старого оборудования. Проведение проверок исправности оборудования.	Неактуальная
2.1.6 Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	2	0,35	Средняя	Низкая	Установлено средство защиты от НСД «Secret Net 7»	Инструкция пользователя, Технологический процесс, Перечень ПДн, Список лиц допущенных к обработке, матрица доступа	Неактуальная

Продолжение Таблицы 1

Наименование угрозы	Y_2	Y	Возможность реализации угрозы	Опасность угрозы	Меры по противодействию угрозе		Актуальность угрозы
					Технические	Организационные	
						система доступа, Положение о защите ПДн, Инструкция администратора, Технический паспорт, Журнал учета машинных носителей, Соглашение о неразглашении.	
2.1.7 Несанкционированное отключение средств защиты	0	0,25	Низкая	Средняя	Дверь в помещение с ИСПДн оборудована замком, помещение оснащено охранной сигнализацией. Произведена соответствующая угрозе настройка СЗИ .	Документы: Инструкция пользователя, Технологический процесс, Перечень ПДн, Список лиц допущенных к обработке, Разрешительная система доступа, Положение о защите ПДн, Инструкция администратора, Технический паспорт, Журнал учета машинных носителей, Соглашение о неразглашении.	Неактуальная
2.2 Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);							
2.2.1 Компьютерные вирусы	2	0,35	Средняя	Низкая	Установлено САВЗ «Kaspersky Endpoint Security 10 для Windows»	Инструкция пользователя, Инструкция администратора безопасности, Технологический процесс, Инструкция по антивирусной защите	Неактуальная
2.2.2 Недекларированные возможности системного ПО и ПО для обработки персональных данных	0	0,25	Низкая	Низкая	Установлено САВЗ «Kaspersky Endpoint Security 10 для Windows»	Сертифицированное ПО	Неактуальная
2.2.3 Установка ПО, не связанного с исполнением служебных обязанностей	2	0,35	Средняя	Низкая	Настройка средств защиты	Инструкция пользователя, Инструкция администратора безопасности	Неактуальная
2.2.4 Наличие аппаратных закладок в приобретаемых ПЭВМ	0	0,25	Низкая	Низкая	Руководством ООО «Завод углеродных и композиционных материалов» данная угроза признана неактуальной.		Неактуальная
2.2.5 Внедрение аппаратных закладок посторонними лицами после начала эксплуатации ИСПДн	0	0,25	Низкая	Низкая	Дверь в помещение оборудована замком, помещение оснащено охранной сигнализацией. Установлено СЗИ от НСД «Secret Net 7»	Порядок пропускного режима, Инструкция администратора, Технологический процесс	Неактуальная
2.2.6 Внедрение аппаратных закладок сотрудниками организации	2	0,35	Средняя	Низкая		Порядок пропускного режима, Инструкция администратора, Технологический процесс	Неактуальная
2.2.7 Внедрение аппаратных закладок обслуживающим персоналом (ремонтными организациями)	2	0,35	Средняя	Низкая		Инструкция администратора, Технологический процесс	Неактуальная

Продолжение Таблицы 1

Наименование угрозы	Y_2	Y	Возможность реализации угрозы	Опасность угрозы	Меры по противодействию угрозе		Актуальность угрозы
					Технические	Организационные	
2.2.8 Внедрение аппаратных устройств, обеспечивающих выход в сети международного информационного обмена	2	0,35	Средняя	Низкая		Инструкция пользователя, инструкция администратора, технологический процесс. Пропускной режим, Матрица доступа	Неактуальная
2.3 Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз не антропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.							
2.3.1 Утрата ключей доступа	0	0,25	Низкая	Средняя		Инструкция пользователя, Инструкция администратора безопасности	Неактуальная
2.3.2 Непреднамеренная модификация (уничтожение) информации сотрудниками	2	0,35	Средняя	Низкая	Настройка средств защиты	Резервное копирование, Инструкция пользователя, Инструкция администратора безопасности	Неактуальная
2.3.3 Непреднамеренное отключение средств защиты	2	0,35	Средняя	Низкая	Доступ к установлению режимов работы средств защиты предоставляется только администратору безопасности	Инструкция пользователя, Инструкция администратора безопасности	Неактуальная
2.3.4 Выход из строя аппаратно-программных средств	2	0,35	Средняя	Низкая	Дверь в помещение оборудована замком, помещение оснащено охранной сигнализацией.	Резервирование	Неактуальная
2.3.5 Сбой системы электроснабжения	2	0,35	Средняя	Низкая	Использование источника бесперебойного питания	Резервное копирование	Неактуальная
2.3.6 Стихийное бедствие	2	0,35	Средняя	Низкая	Здание оборудовано пожарной сигнализацией		Неактуальная
2.4 Угрозы преднамеренных действий внутренних нарушителей							
2.4.1 Доступ к информации, её модификация и уничтожение сотрудниками, не допущенными к ее обработке	0	0,25	Низкая	Средняя	Установлено средства защиты от НСД «Secret Net 7»	Разрешительная система доступа, Технологический процесс	Неактуальная
2.4.2 Разглашение, модификация и уничтожение информации сотрудниками, допущенными к ее обработке	2	0,35	Средняя	Низкая	Установлено средства защиты от НСД «Secret Net 7»	Инструкция пользователя, Резервное копирование	Неактуальная
2.4.3 Копирование информации на неучтенные внешние машинные носители	2	0,35	Средняя	Низкая	Установлено СЗИ от НСД «Secret Net 7», Запрет на подключение неучтенных съемных носителей в настройках СЗИ	Разрешительная система допуска, Технологический процесс, Журнал учета машинных носителей	Неактуальная
2.4.4 Перехват управления загрузкой с изменением необходимой технологической информации для получения НСД в операционную среду ИСПДн	0	0,25	Низкая	Средняя	Применение аппаратной части СЗИ от НСД «Secret Net 7», Матрица доступа	Инструкция пользователя, Ограничение физического доступа посторонних лиц	Неактуальная

Продолжение Таблицы 1

Наименование угрозы	Y_2	Y	Возможность реализации угрозы	Опасность угрозы	Меры по противодействию угрозе		Актуальность угрозы
					Технические	Организационные	
2.5 Угрозы несанкционированного доступа по каналам связи со стороны нарушителей, не имеющих доступ к ИСПДн							
2.5.1 Несанкционированный доступ через сети международного обмена	0	0,25	Низкая	Средняя	Установлен МЭ «Программный комплекс С-Терра Клиент Версия 4.1»	Технологический процесс, Инструкция пользователя, Инструкция администратора безопасности	Неактуальная
2.5.2 Несанкционированный доступ через ЛВС организации	2	0,35	Средняя	Низкая		Технологический процесс, Инструкция пользователя, Инструкция администратора безопасности	Неактуальная
2.5.3 Анализ сетевого трафика с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации	2	0,35	Средняя	Низкая		Сеть физически отделена от сетей международного обмена	Неактуальная
2.5.4 Сканирование, направленное на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.	2	0,35	Средняя	Низкая		Сеть физически отделена от сетей международного обмена	Неактуальная
2.5.5 Угрозы выявления паролей	0	0,25	Низкая	Средняя	Дверь оборудована замком, помещение оснащено охранной сигнализацией. Установлено СЗИ от НСД «Secret Net 7»	Инструкция администратору, Инструкция пользователям	Неактуальная
2.5.6 Угрозы получения НСД путем подмены доверенного объекта при сетевом доступе	0	0,25	Низкая	Средняя	Установлены МЭ «Программный комплекс С-Терра Клиент Версия 4.1», САВЗ «Kaspersky Endpoint Security 10 для Windows»	Инструкции пользователя и администраторам	Неактуальная
2.5.7 Угрозы типа «Отказ в обслуживании»	0	0,25	Низкая	Низкая	Динамическое распределение нагрузки, Избыточность каналов связи и вычислительных мощностей	Описание технологического процесса, Инструкция администратору	Неактуальная
2.5.8 Внедрение по сети вредоносных программ	2	0,35	Средняя	Низкая	Установлено САВЗ «Kaspersky Endpoint Security 10 для Windows»	Инструкция администратору, Инструкция пользователям	Неактуальная
2.5.9 Утечка атрибутов доступа	2	0,35	Средняя	Низкая	Установлено средства защиты от НСД «Secret Net 7»	Технологический процесс, Инструкция пользователя, Инструкция администратора безопасности	Неактуальная
2.6 Угрозы перехвата при передаче по проводным (кабельным) линиям связи							
2.6.1 Перехват за переделами контролируемой зоны	2	0,35	Средняя	Низкая	Установлено СКЗИ «ПК С-Терра Клиент Версия 4.1»	Технологический процесс	Неактуальная
2.6.2 Перехват в пределах контролируемой зоны внешними нарушителями	0	0,25	Низкая	Средняя		Пропускной режим Технологический процесс	Неактуальная

Продолжение Таблицы 1

Наименование угрозы	Y_2	Y	Возможность реализации угрозы	Опасность угрозы	Меры по противодействию угрозе		Актуальность угрозы
					Технические	Организационные	
2.6.3 Перехват в пределах контролируемой зоны внутренними нарушителями	2	0,35	Средняя	Низкая		Технологический процесс, Матрица доступа	Неактуальная

Таким образом, в отношении персональных данных, обрабатываемых в ИСПДн «Бухгалтерия» Общества с ограниченной ответственностью «Завод углеродных и композиционных материалов» актуальные угрозы не выявлены.

Комиссия в составе:

Председатель комиссии _____ К.С. Рыжов

Члены комиссии _____ А.С. Жаворонкин

_____ А.Ф. Морар

ПРИЛОЖЕНИЕ И

СОГЛАСОВАНО

Руководитель органа по аттестации
объектов информатизации
ЗАО «Гранит Информ»

_____ Н.В. Узбеков
«_____»_____ 2018 г.

УТВЕРЖДАЮ

Исполнительный директор Общества с ограниченной ответственностью «Завод углеродных и композиционных материалов»

_____ С.А. Подкопаев
«_____»_____ 2018 г.

Общество с ограниченной ответственностью
«Завод углеродных и композиционных материалов»
г. Челябинск, Челябинский электродный завод

МЕРЫ
по обеспечению безопасности персональных данных при их обработке
в информационной системе персональных данных
«Бухгалтерия»

2018 г.

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Данные требования по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных «Бухгалтерия» Общества с ограниченной ответственностью «Завод углеродных и композиционных материалов» (далее ИСПДн) разработаны на основании Приказа № 21 «О составе и содержании организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утверждённого 18 февраля 2013 г. директором ФСТЭК России, и «Частной модели угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Бухгалтерия» Общества с ограниченной ответственностью «Завод углеродных и композиционных материалов» № 06-33/56дсп от 21.04.2018 г.

1.2 Требования определяют совокупность организационных и технических мероприятий, необходимых для обеспечения заданного уровня безопасности персональных данных при их обработке в ИСПДн. Требования распространяются только на данную ИСПДн.

2 ОРГАНИЗАЦИОННЫЕ МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

- должны быть предусмотрены меры физической охраны помещений ИСПДн для предотвращения бесконтрольного доступа в помещения посторонних лиц;
- доступ в помещения ИСПДн посторонним лицам должен быть разрешён только в присутствии сотрудников, допущенных к обработке ПДн;
- доступ к техническим средствам ИСПДн должен быть разрешён только тем сотрудникам, которым он нужен для выполнения служебных обязанностей;
- закупка технических средств должна осуществляться только у производителей или их официальных представителей;
- пользователи ИСПДн должны обладать минимально необходимыми правами доступа в системе, обязанности по соответствующей настройке системы разграничения доступа возлагаются на администратора ИСПДн;
- доступ к персональным данным должен предоставляться сотрудникам в соответствии с утверждённым списком;
- доступ к персональным данным и иным защищаемым ресурсам ИСПДн должен предоставляться в соответствии с утверждённой матрицей доступа;
- ИСПДн должна быть физически или логически отделена от локальной сети организации, требования по соответствующей настройке рабочих станций и коммутационного оборудования возлагаются на администратора ИСПДн;
- ИСПДн должна быть физически отделена от сетей связи общего пользования межсетевым экраном.

3 МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

В комплекс мер по защите персональных данных (далее – ПДн) при их обработке в ИСПДн от несанкционированного доступа (далее НСД) и неправомерных действий входят следующие направления:

3.1 Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)

- Идентификация и аутентификация пользователей, являющихся работниками оператора;
- Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов;

- Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;
- Защита обратной связи при вводе аутентификационной информации;
- Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей);

3.2 Управление доступом субъектов доступа к объектам доступа (УПД)

- Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей;
- Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа;
- Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами;
- Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы;
- Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы;
- Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе);
- Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети;
- Регламентация и контроль использования в информационной системе технологий беспроводного доступа;
- Регламентация и контроль использования в информационной системе мобильных технических средств;
- Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы);

3.3 Регистрация событий безопасности (РСБ)

- Определение событий безопасности, подлежащих регистрации, и сроков их хранения;
- Определение состава и содержания информации о событиях безопасности, подлежащих регистрации;
- Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;
- Защита информации о событиях безопасности;

3.4 Антивирусная защита (АВЗ)

- Реализация антивирусной защиты;
- Обновление базы данных признаков вредоносных компьютерных программ (вирусов);

3.5 Контроль (анализ) защищенности персональных данных (АНЗ)

- Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации;

3.6 Защита среды виртуализации (ЗСВ)

- Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации;
- Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин;

3.7 Защита технических средств (ЗТС)

- 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, в помещения и сооружения, в которых они установлены;
- Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр;

3.8 Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)

- Обеспечение защиты персональных данных 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;

Комиссия в составе:

Председатель комиссии _____ К.С. Рыжов

Члены комиссии _____ А.С. Жаворонкин

_____ А.Ф. Морар

ПРИЛОЖЕНИЕ К

СОГЛАСОВАНО

Руководитель органа по аттестации
объектов информатизации
АО «Гранит Информ»

_____ Н.В. Узбеков
«_____»_____ г.Челябинск

УТВЕРЖДАЮ

Исполнительный директор Общества
с ограниченной ответственностью «Завод
углеродных и композитных материалов»

_____ С.А. Подкопаев
«_____»_____ г.Челябинск

Общество с ограниченной ответственностью «Завод углеродных и композитных материалов»
г. Челябинск, Челябинский электродный завод.

МОДЕЛЬ ПОТЕНЦИАЛЬНОГО НАРУШИТЕЛЯ
информационной системы персональных данных
«Бухгалтерия»

г. Челябинск

УГРОЗЫ, НЕ ЯВЛЯЮЩИЕСЯ АТАКОЙ

1.1 Угрозы, не связанные с деятельностью человека:

– землетрясения;
– наводнения;
– ураганы.

1.2 Угрозы социально–политического характера:

– забастовки;
– саботаж;
– локальные конфликты.

1.3 Ошибочные действия и (или) нарушения тех или иных требований лицами, санкционировано взаимодействующими с возможными объектами угроз:

– непредумышленное искажение или удаление программных компонентов АСЗИ;
– внедрение и использование неучтенных программ;
– игнорирование организационных ограничений (установленных правил) при работе с ресурсами АСЗИ, включая средства защиты информации. В частности:
- нарушение правил хранения информации ограниченного доступа, используемой при эксплуатации средств защиты информации (в частности, ключевой, парольной и аутентифицирующей информации);
- предоставление посторонним лицам возможности доступа к средствам защиты информации, а также к техническим и программным средствам, способным повлиять на выполнение предъявляемых к средствам защиты информации требований;
- настройка и конфигурирование средств защиты информации, а также технических и программных средств, способных повлиять на выполнение предъявляемых к средствам защиты информации требований, в нарушение нормативных и технических документов;
- несообщение о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа.

1.4 Угрозы техногенного характера:

– аварии (отключение электропитания, системы заземления, разрушение инженерных сооружений и т.д.);
– неисправности, сбои аппаратных средств, нестабильность параметров системы электропитания, заземления и т.д.;
– помехи и наводки, приводящие к сбоям в работе аппаратных средств.

1 АТАКИ НА ЭТАПЕ ЭКСПЛУАТАЦИИ ТЕХНИЧЕСКИХ И ПРОГРАММНЫХ СРЕДСТВ КРИПТОСРЕДСТВА И СФК

2.1 Модель нарушителя.

Нарушитель:

Предполагается, что потенциальный нарушитель не имеет права доступа в контролируемую зону информационной системы.

Примечание:

Операторы ПК в силу своих должностных обязанностей изначально имеют доступ к защищаемым персональным данным и конфиденциальной информации и не могут рассматриваться как потенциальные нарушители.

Администратор ИБ, обладает всей полнотой информации об информационной системе, применяемых средствах и методах защиты, осуществляют техническое обслуживание программных и технических средств криптосредства и СФК, включая их настройку, конфигурирование и распределение ключевой документации между непривилегированными пользователями.

Администратор ИБ относится к категории привилегированных пользователей информационной системы, которые назначаются из числа особо доверенных лиц и не рассматривается в качестве потенциального нарушителя.

Объект атаки:

- документация на криптосредство и на технические и программные компоненты СФК;
- защищаемые персональные данные и конфиденциальная информация;
- ключевая, аутентифицирующая и парольная информация;
- криптографически опасная информация (КОИ);
- криптосредство (программные компоненты криптосредства);
- технические и программные компоненты СФК;
- данные, передаваемые на машинных носителях информации;
- помещения, в которых находятся защищаемые ресурсы информационной системы.

Цель атаки:

Целями атаки являются нарушение целостности, доступности и конфиденциальности защищаемых персональных данных и конфиденциальной информации, а также создание условий, способствующих таким нарушениям.

***Имеющаяся у нарушителя информация об объекте атаки*:**

Предполагается, что потенциальные нарушители для подготовки и проведения атак могут обладать следующей информацией:

– содержание технической документации на технические и программные компоненты СФК.

Примечание:

Предполагается, что потенциальные нарушители:

– не обладают информацией о долговременных ключах криптосредства, т.к. указанные сведения являются информацией ограниченного распространения.

– не обладают наряду с доступными в свободной продаже документацией на криптосредство и СФК исходными текстами прикладного программного обеспечения;

– не обладают возможными данными, передаваемыми в открытом виде по каналам связи, не защищенным от НСД к информации организационно-техническими мерами (фазовые пуски, синхропосылки, незашифрованные адреса, команды управления и т.д.), сведениями о линиях связи, по которым передается защищаемая информация; информацией о всех проявляющихся в каналам связи неисправностях и сбоях технических средств СФК, нарушениях правил эксплуатации криптосредства и СФК по причине отсутствия каналов связи;

– не могут получить сведения, в результате анализа ПЭМИН от технических средств СФК, т.к. технические средства расположены в пределах контролируемой зоны и удовлетворяют требованиям государственных стандартов на электромагнитную совместимость.

Имеющиеся у нарушителя средства атаки:

Предполагается, что потенциальные нарушители располагают:

- доступными в свободной продаже аппаратными компонентами СФК;
- доступными в свободной продаже техническим средствами и ПО;
- располагают специально разработанным программным обеспечением.

Примечание:

Предполагается, что потенциальные нарушители не могут располагать штатными средствами информационной системы, которые расположены в пределах контролируемой зоны.

Канал атаки:

- машинные носители информации;
- носители информации, выведенные из употребления;
- канал утечки за счет электронных устройств негласного получения информации.

Определение типа нарушителя:

Исходя из вышеперечисленных предполагаемых характеристик потенциального нарушителя на основании документа «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных и конфиденциальной информации при их обработке в автоматизированной системе» (утвержден руководством 8 Центра ФСБ России 21 февраля 2008 года № 149/54-144) потенциальному нарушителю присвоен тип **Н1** и для информационной системы должна быть обеспечена специальная криптографическая защита по уровню **КС1.**

Комиссия в составе:

Председатель комиссии _____ К.С. Рыжов

Члены комиссии _____ Жаворонкин А.С.

_____ Морар А.Ф.

ПРИЛОЖЕНИЕ Л

УТВЕРЖДАЮ

Исполнительный директор Общества с ограниченной ответственностью «Завод углеродных и композитных материалов»

_____С.А. Подкопаев
«____» _____ 2018 г.

Общество с ограниченной ответственностью «Завод углеродных и композитных материалов»
г. Челябинск, Челябинский электродный завод

ИНСТРУКЦИЯ
по эксплуатации средств защиты информации
в информационной системе персональных данных
«Бухгалтерия»

2018 г.

Перед обработкой защищаемой информации необходимо убедиться, что все средства защиты информации включены и работают исправно.

При использовании средств защиты информации в ИСПДн следует руководствоваться следующими документами, поставляемыми в комплекте с СЗИ:

1. **Средство межсетевого экранирования «С-Терра Клиент Версия 4.1»**

При эксплуатации системы выполнять требования и руководствоваться требованиями:

– «С-Терра Клиент. Руководство администратора»;
– «С-Терра Клиент. Руководство пользователя».

2. **Средство защиты информации от несанкционированного доступа «Secret Net 7»**

При эксплуатации системы выполнять требования и руководствоваться требованиями:

– «Средство защиты информации Secret Net 7. Руководство пользователя»;
– «Средство защиты информации Secret Net 7. Руководство администратора. Принципы построения»;
– «Средство защиты информации Secret Net 7. Руководство администратора. Установка, обновление и удаление»;
– «Средство защиты информации Secret Net 7. Руководство администратора. Локальная работа с журналами регистрации»;
– «Средство защиты информации Secret Net 7. Руководство администратора. Работа с программой оперативного управления»;
– «Средство защиты информации Secret Net 7. Руководство администратора. Настройка механизмов защиты».

3. **Средство антивирусной защиты «Kaspersky Endpoint Security 10 для Windows»**

– «Kaspersky Endpoint Security 10 для Windows. Руководство пользователя»;
– «Kaspersky Endpoint Security 10 для Windows. Руководство администратора».

4. **Средство криптографической защиты информации «С-Терра Клиент Версия 4.1»**

При эксплуатации системы выполнять требования и руководствоваться требованиями:

– «С-Терра Клиент. Руководство администратора»;
– «С-Терра Клиент. Руководство пользователя».

Ответственный за обеспечение безопасности персональных данных, Руководитель направления обеспечения безопасности – специалист по защите информации _____ Омельченко А.М.

ПРИЛОЖЕНИЕ М

УТВЕРЖДАЮ
Исполнительный директор Общества с ограниченной ответственностью «Завод углеродных и композиционных материалов»

_____ С.А. Подкопаев
«____» _____ 2018 г.

ТЕХНИЧЕСКИЙ ПАСПОРТ
на объект информатизации
«Бухгалтерия»
Общества с ограниченной ответственностью
«Завод углеродных и композиционных материалов»

СОСТАВИЛ
Техник АО «Гранит Информ»
_____ А.Ф. Морар

«____» _____ 2018 г.

2018 г.

1 ОБЩИЕ СВЕДЕНИЯ ОБ ОБЪЕКТЕ

1.1 Наименование объекта: «Бухгалтерия» Общества с ограниченной ответственностью «Завод углеродных и композиционных материалов».

1.2 Расположение объекта: г. Челябинск, Челябинский электродный завод, Бухгалтерия

1.3 Классификация объекта.

Уровень защищенности: 4 (**4 УЗ**), «Акт присвоения уровня защищенности…» № 06-33/60дсп от 21.04.2018 г.;

2 СОСТАВ ОБОРУДОВАНИЯ ОБЪЕКТА

2.1 Состав основных технических средств и систем (ОТСС) объекта информатизации отражен в таблице 2.1.

Таблица 2.1 - **Перечень ОТСС, входящих в состав ОИ «Бухгалтерия»**

№	Тип	Модель	Заводской / инвентаризационный номер
1	Системный блок	HP PRO 3500	RUA31706ZG
2	НЖМД	ST500DM002-1BD142	Z3TEDYW1
3	Монитор	HP 2011x	CNC128RQ3K
4	Клавиатура	HP PR1101U	BAUWF11RZ1I911
5	Мышь	Genius NetScroll 100X	X75891203592
6	Принтер	Ricoh SP 3510SF/Aficio SP 3510SF	T333Q201268
7	Флешкарта	Smartbuy 4Gb	90005A612A3BF021
8	Флешкарта	Kingmax PI-03G2 8Gb	3HAC0381400000352
9	ИБП	APC Back-UPS CS 500	4B1137P05147
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			

1.1 Схема размещения и расположения ОТСС на объекте с привязкой к границам контролируемой зоны.

Структура, топология и размещение ОТСС и ВТСС объекта относительно границ контролируемой зоны объекта приведены на рисунках 2.1 – 2.3.

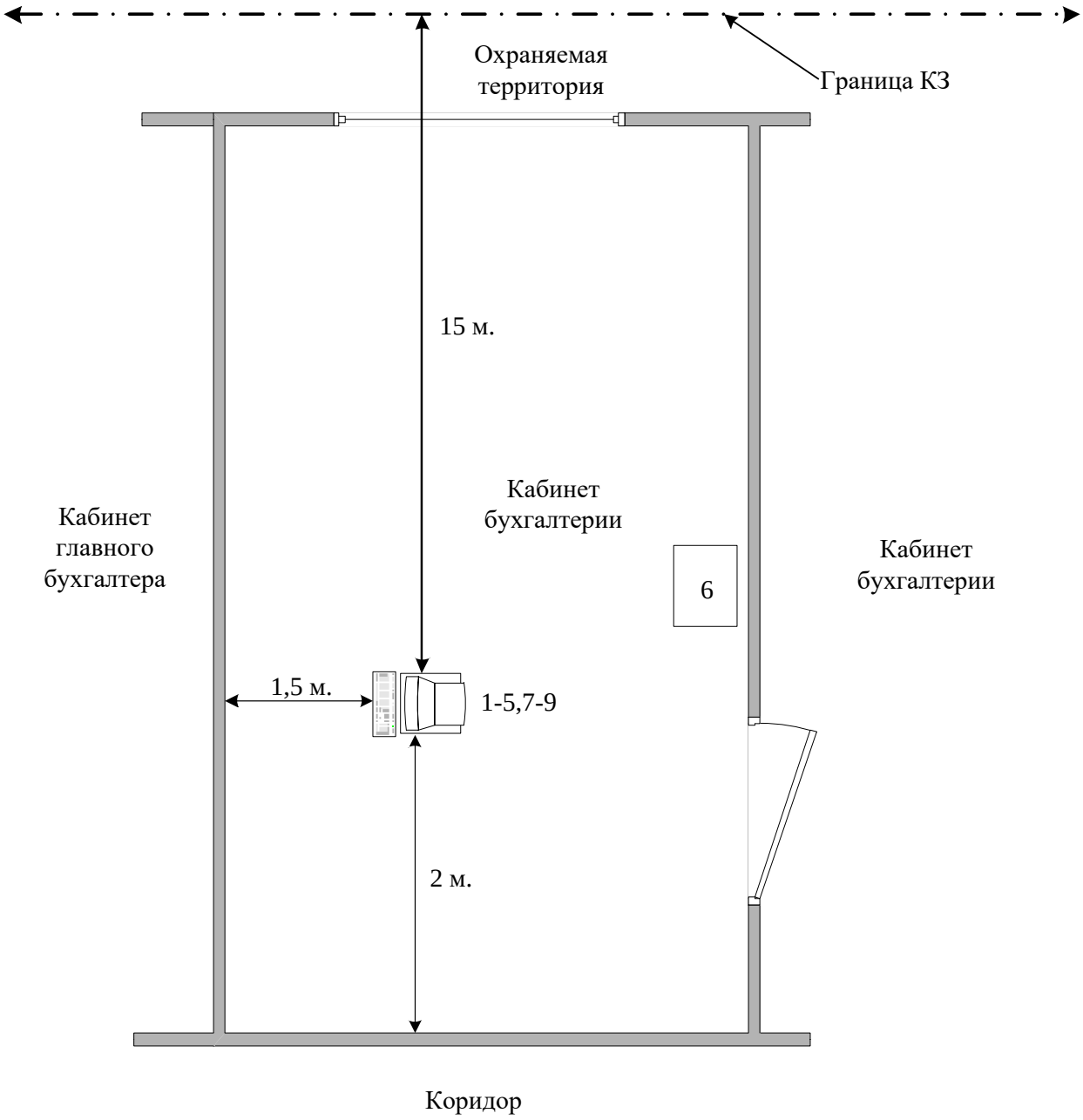

Рисунок 2.1 – Размещение ОТСС «Бухгалтерия» относительно границ контролируемой зоны

*Примечание: Обозначения 1-9 приведены в Таблице 2.1 основной части технического паспорта.

Контролируемой зоной является охраняемая территория Общества с ограниченной ответственностью «Завод углеродных и композиционных материалов» по адресу: г. Челябинск, Челябинский электродный завод. Граница контролируемой зоны определена приказом «Об определении границ контролируемой зоны…» № 349 от 16.03.2018.

Минимальное расстояние от ОТСС до КЗ составляет 15 метров.

Размещение ВТСС приведено на рисунке 2.2.

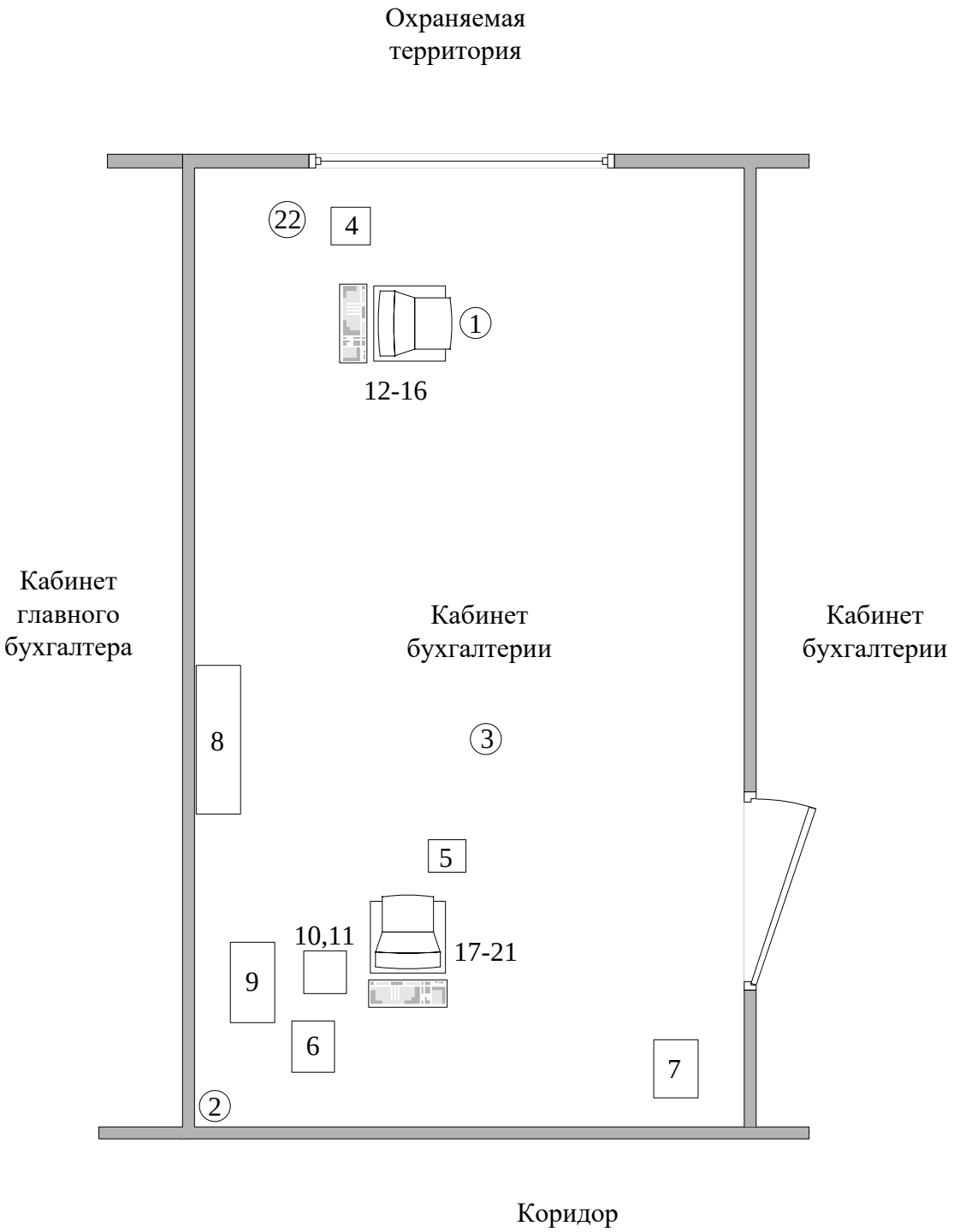

Рисунок 2.2 – Размещение ВТСС «Бухгалтерия»
*Примечание: Обозначения 1-22 приведены в Таблице 2.2 основной части технического паспорта.

Размещение ВТСС, системы электропитания, заземления и инженерных коммуникаций приведено на рисунке 2.3.

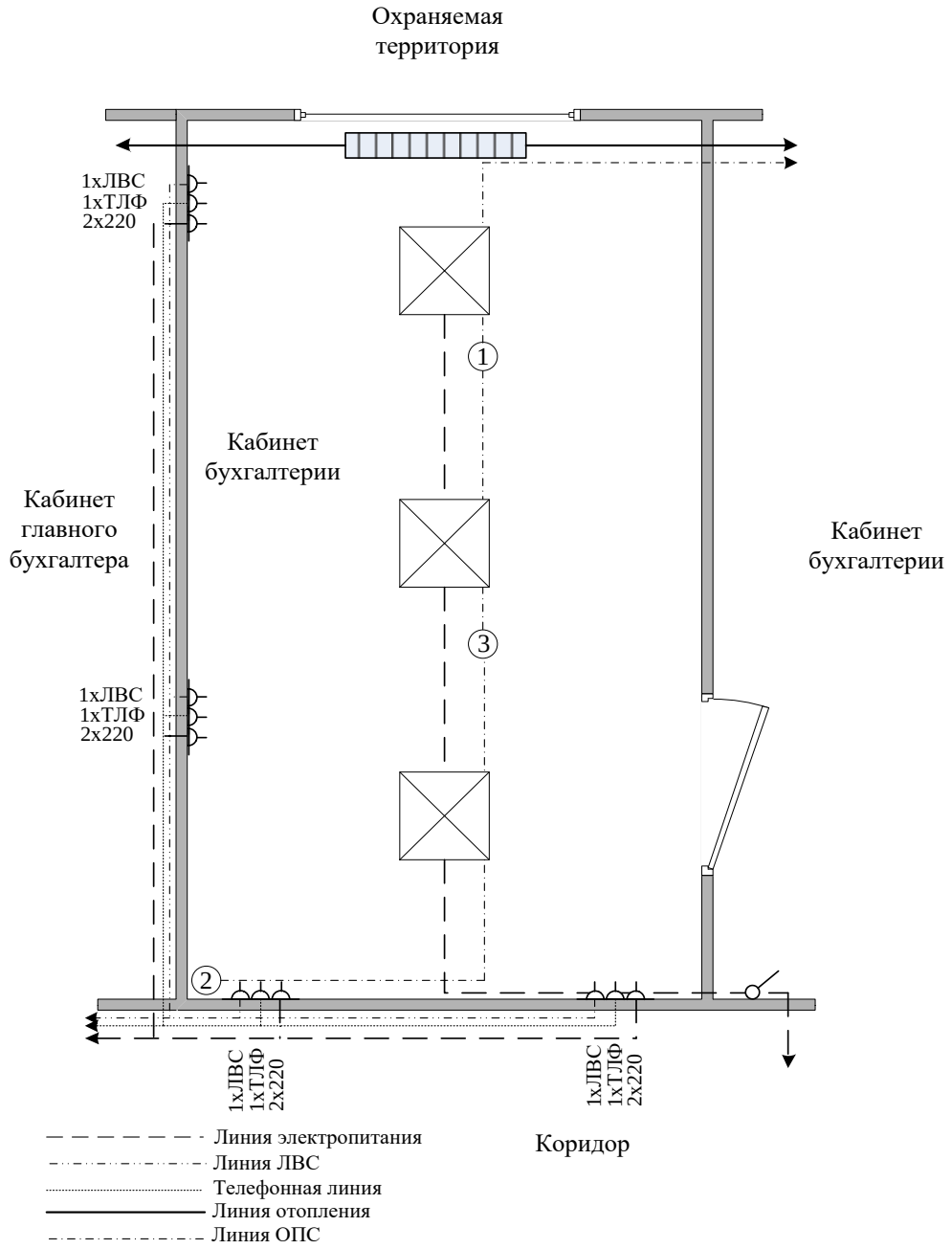

Рисунок 2.3 – Размещение системы электропитания, заземления и инженерных коммуникаций

*Примечание: Обозначения 1-3 приведены в Таблице 2.2 основной части технического паспорта.

Наименование линии	**Выходит за пределы КЗ (выходит/не выходит)**
Линия электропитания	не выходит
Линия заземления	не выходит
Линия охранной сигнализации	не выходит
Линия пожарной сигнализации	не выходит
Линия телефонной связи	не выходит
Линия ЛВС	не выходит
Линия отопления	не выходит

2.2 Перечень средств защиты информации, установленных на объекте информатизации «Бухгалтерия» приведен в Таблице 2.3.

Таблица 2.3 - **Перечень средств защиты, установленных на ОИ «АРМ 2»**

№ п /п	Наименование и тип средства защиты информации	Заводской номер, СЗЗ	Сведения о сертификате
1.	СЗИ от НСД «Secret Net 7»	GL83EB81, Л 643287	№ 2707 от 07.09.2012 г.
2.	МЭ «Программный комплекс С-Терра Клиент Версия 4.1»	106096, К 169207	№ 3371 от 27.03.2015 г., № СФ/515-2659 от 20.07.2015 г.
3.	СКЗИ «Программный комплекс С-Терра Клиент Версия 4.1»	106096, К 169207	№ 3371 от 27.03.2015 г., № СФ/114-2513 от 01.12.2014 г.
4.	САВЗ «Kaspersky Endpoint Security 10 для Windows»	СМП8069-8854, Л 874356	№ 3025 от 25.11.2013 г.

2.3 Перечень программных средств, установленных на объекте вычислительной техники «АРМ 2» приведен в Таблице 2.4**:**

Таблица 2.4 – **Перечень ПО установленного на ОИ «АРМ 2»**

	Наименование ПО	Версия
1	7-Zip	9.20.00.0
2	ABBYY FineReader 12 Corporate	12.1.609
3	Adobe Acrobat Reader DC	15.023.20053
4	Microsoft Office Professional Plus 2016	16.0.4266.1001
5	КОМПАС-3D Viewer	16.1
6	КриптоПро CSP	3.6.7777

3 СВЕДЕНИЯ О СООТВЕТСТВИИ ОТСС ОБЪЕКТА ВТ ТРЕБОВАНИЯМ ПО БЕЗОПАСНОСТИ ИНФОРМАЦИИ

3.1 Протоколы испытаний и даты их регистрации

3.2 Сведения об аттестации объекта информатизации на соответствие требованиям по безопасности информации:

4 УЧЕТ ПРОВЕДЕНИЯ РЕГЛАМЕНТНЫХ ПРОВЕРОК

Таблица 4.1 - Учет проведения регламентных проверок

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

5 ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Таблица 5.1 - Лист регистрации изменения состава и размещения ОТСС, ВТСС и средств защиты объекта информатизации

№ п/п Дата введения изменений	Наименование документа, фиксирующего изменения	№ замененных (исправленных) листов формуляра	Подпись лица, внесшего изменения

ПРИЛОЖЕНИЕ Н

АКЦИОНЕРНОЕ ОБЩЕСТВО
ГРАНИТ ИНФОРМ
454006, г. Челябинск, ул. Красноармейская, 55
тел (351) 218 28 28, эл. почта: info@g-inform.ru

УТВЕРЖДАЮ

Руководитель органа по аттестации объектов информатизации
АО «Гранит Информ»

_____ Н.В. Узбеков

«_____»_____ 2018 г.

ЗАКЛЮЧЕНИЕ № ГИ. 2018.00872
ПО РЕЗУЛЬТАТАМ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ

Объект информатизации
информационная система персональных данных
«Бухгалтерия»
Общества с ограниченной ответственностью
«Завод углеродных и композиционных материалов»
г. Челябинск, Челябинский электродный завод

2018 г.

ОБЩИЕ ПОЛОЖЕНИЯ

Аттестационная комиссия, сформированная ЗАО «Гранит Информ», действующая на основании Аттестата аккредитации № СЗИ RU.1960.B167.326 (действителен до 01.02.2020 г.) в составе экспертов по соответствующим направлениям:

Рыжов К.С. – заместитель генерального директора АО «Гранит Информ», председатель комиссии;

Жаворонкин А.С. – ответственный за соответствие требованиям по организационно – техническому направлению, главный инженер АО «Гранит Информ», член комиссии;

Морар А.Ф. – ответственный за проведение аттестационных испытаний на соответствие требованиям по защите информации по каналам НСД, техник АО «Гранит Информ», член комиссии;

провела аттестационные испытания в соответствии с «Программой и методикой проведения аттестационных испытаний объекта информатизации информационной системы персональных данных» (уч. № 3438дсп от 23.03.2018 г.). Результаты аттестационных испытаний приведены в протоколах по направлениям:

проверка объекта на соответствие организационно-техническим требованиям;

защита от несанкционированного доступа;

Аттестационные испытания проведены в рамках аттестации информационных систем персональных данных, в соответствии с приказом ФСТЭК России № 21 от 18 февраля 2013 г. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», «Положением по аттестации объектов информатизации на соответствие требованиям безопасности информации», а также других действующих нормативно-методических документов ФСТЭК России.

Заявитель аттестационных испытаний объекта – Общество с ограниченной ответственностью «Завод углеродных и композиционных материалов».

2 ЦЕЛЬ, ОБЪЕКТЫ И УСЛОВИЯ ИСПЫТАНИЙ

2.1 Цель испытаний: оценка соответствия принятых организационно-технических мер по обеспечению безопасности персональных данных действующим требованиям нормативно-правовых документов по защите информации, а том числе:

– «Постановление об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», утвержденного постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119;

– Приказ ФСТЭК России от 13 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».

2.2 Объект аттестационных испытаний – объект информатизации информационная система персональных данных, размещенная по адресу: г. Челябинск, Челябинский электродный завод, 5 этаж, Бухгалтерия (далее ИСПДн).

2.3 Состав основных технических средств и систем (ОТСС) объекта приведен в таблице 2.1. Состав средств защиты информации объекта приведен в таблице 2.2. Полное описание объекта, состав вспомогательных технических средств и систем (ВТСС), расположение ВТСС относительно ОТСС и пр. параметры приведены в «Техническом паспорте» (№ 06-33/61дсп от 21.04.2018 г.).

Таблица 2.1 - **Состав ОТСС ИСПДн «Бухгалтерия»**

№ п/п	Наименование технического средства	Модель	Заводской (инвентарный) номер
1	Системный блок	HP PRO 3500	RUA31706ZG
2	НЖМД	ST500DM002-1BD142	Z3TEDYW1
3	Монитор	HP 2011x	CNC128RQ3K
4	Клавиатура	HP PR1101U	BAUWF11RZ1I911
5	Мышь	Genius NetScroll 100X	X75891203592
6	Принтер	Ricoh SP 3510SF/Aficio SP 3510SF	T333Q201268
7	Флешкарта	Smartbuy 4Gb	90005A612A3BF021
8	Флешкарта	Kingmax PI-03G2 8Gb	3HAC0381400000352
9	ИБП	APC Back-UPS CS 500	4B1137P05147

Таблица 2.2– **Перечень СЗИ «Бухгалтерия»**

№ п/п	Наименование СЗИ	Модель	Заводской номер	СЗЗ	Сведения о сертификате
1	СЗИ от НСД	Secret Net 7	GL83EB81	Л 643287	Сертификат ФСТЭК № 2707 действителен до 07.09.2018 г.
2	СКЗИ	Программный комплекс С-Терра Клиент Версия 4.1	106096	К 169207	Сертификат ФСТЭК № 3371 действителен до 27.03.2021 г., Сертификат ФСБ № СФ/114-3227 действителен до 15.01.2019 г.
3	Антивирус	Kaspersky Endpoint Security 10 для Windows	СМП8069-8854	Л 874356	Сертификат ФСТЭК № 3025 действителен до 25.11.2019 г.

№ п/п	Наименование СЗИ	Модель	Заводской номер	СЗЗ	Сведения о сертификате
4	Межсетевой экран	Программный комплекс С-Терра Клиент Версия 4.1	106096	К 169207	Сертификат ФСТЭК № 3371 действителен до 27.03.2021 г., Сертификат ФСБ № СФ/515-3227 действителен до 15.01.2019 г.

2.4. В ходе аттестационных испытаний проводились следующие мероприятия:

– проверка объекта информатизации на соответствие организационно-техническим требованиям по защите информации;

– проверка ИСПДн на соответствие требованиям по защите информации от несанкционированного доступа;

– подготовка отчетной документации и оценка результатов испытаний объекта информатизации.

2.5. При проведении аттестационных испытаний применялись следующие методы проверок и испытаний:

– экспертно-документальный метод, предусматривающий проверку соответствия ИСПДн требованиям по безопасности информации на основании экспертной оценки полноты и достаточности представленных документов по обеспечению необходимых мер защиты информации в ИСПДн, а также соответствия реальных условий эксплуатации требованиям по размещению, монтажу и эксплуатации ИСПДн;

– проверка функций или комплекса функций защиты информации от НСД с помощью тестирующих средств, а также путем пробного запуска средств защиты информации от НСД и наблюдения за их выполнением;

2.6. В ходе проведения аттестационных испытаний использовались следующие руководящие и нормативно-технические документы:

– «Положение по аттестации объектов информатизации по требованиям безопасности информации», утвержденное председателем Гостехкомиссии России 25 ноября 1994 г.

– «Постановление об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», утвержденного постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119.

– Приказ ФСТЭК России от 13 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».

– Руководящий документ Гостехкомиссии России. «Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации», утвержден председателем Гостехкомиссии России от 25 июля 1997 г.

– Руководящий документ Гостехкомиссии России. «Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности информации», утвержден председателем Гостехкомиссии России от 30 марта 1992 г.

– Руководящий документ Гостехкомиссии России. «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» Приказ Председателя Гостехкомиссии России от 04 июня 1999 г. № 114.

2.7. При проведении аттестационных испытаний использовалась программные и технические средства, указанные в таблице 2.3.

Таблица 2.3 - **Используемые программные и технические средства**

Тип средства измерений	**Наименование**	**Заводской номер**	**Дата очередной поверки**
Программа поиска и гарантированного уничтожения информации на дисках	«TERRIER» **(**версия 3.0)	Голограмма № А 293818	Сертификат ФСТЭК № 1193, действ. до 16.05.2018 г.
Программа фиксации и контроля исходного состояния программного комплекса	«ФИКС» (версия 2.0.1)	Голограмма № А 267757	Сертификат ФСТЭК № 913, действ. до 01.06.2019 г.
Средство создания модели системы разграничения доступа	«Ревизор 1 XP»	Голограмма № А 296220	Сертификат ФСТЭК № 989, действ. до 08.02.2020 г.
Программа контроля полномочий доступа к информационным ресурсам	«Ревизор 2 XP»	Голограмма № А 268720	Сертификат ФСТЭК № 990, действ. до 08.02.2020 г.
Программа поиска и контроля уязвимостей в вычислительных сетях	Сетевой сканер «Ревизор сети» версия 3.0	Голограмма № З 263216	Сертификат ФСТЭК № 3413, действ. до 02.06.2018 г.

3 ПОРЯДОК ПРОВЕДЕНИЯ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ

Для проведения испытаний аттестационной комиссии предъявлены следующие исходные данные и документация (см. таблица 3.1):

Таблица 3.1 - **Исходные данные на объект информатизации**

№ п.п.	Требовалось по «Программе аттестационных…»	Предоставлено Заявителем	Рег. номер документа
1	Технический паспорт на объект вычислительной техники	Технический паспорт на ИСПДн	№ 06-33/61дсп от 21.03.2018 г.
	Планы размещения ОТСС и ВТСС		
	Схемы прокладки линий передачи данных ОТСС и ВТСС		
	Состав и схемы размещения средств защиты информации		
	Схемы и характеристики систем электропитания и заземления ОТСС и ВТСС		
	Состав технических и программных средств, входящих в ИСПДн		
	Состав общесистемного и прикладного ПО		
2	Перечень защищаемой информации	Перечень персональных данных подлежащих защите в информационных системах персональных данных	б/н от 21.03.2018 г.
3	Организационно-распорядительная документация разрешительной системы доступа персонала к защищаемым ресурсам ИСПДн	Приказ об организации работ по обеспечению безопасности персональных данных в информационных системах персональных данных	№ 350 от 16.03.2018 г.
4		Разрешительная система доступа пользователей к защищаемым информационным ресурсам информационной системы персональных данных «Бухгалтерия» Общества с ограниченной ответственностью «Завод углеродных и композиционных материалов»	№ 06-33/54дсп от 21.03.2018 г.

№ п.п.	Требовалось по «Программе аттестационных…»	Предоставлено Заявителем	Рег. номер документа
5	Акт классификации ИСПДн	Акт присвоения уровня защищенности ИСПДн «Бухгалтерия» Общества с ограниченной ответственностью «Завод углеродных и композиционных материалов»	№ 06-33/60дсп от 21.03.2018 г.
6		Акт классификации АС «Бухгалтерия» Общества с ограниченной ответственностью «Завод углеродных и композиционных материалов»	№ 06-33/59дсп от 21.03.2018 г.
7	Модель угроз безопасности информации	Частная модель угроз безопасности персональных данных «Бухгалтерия» Общества с ограниченной ответственностью «Завод углеродных и композиционных материалов»	№ 06-33/56дсп от 21.03.2018 г.
8	Требования по обеспечению безопасности информации	Меры по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных «Бухгалтерия» Общества с ограниченной ответственностью «Завод углеродных и композиционных материалов»	№ 06-33/62дсп от 21.03.2018 г.
9	Организационная документация	Приказ об организации работ по обеспечению безопасности персональных данных в информационных системах персональных данных	№ 350 от 16.03.2018 г.
10		Описание технологического процесса обработки информации в информационной системах персональных данных «Бухгалтерия» Общества с ограниченной ответственностью «Завод углеродных и композиционных материалов»	№ 06-33/53дсп от 21.03.2018 г.

№ п.п.	Требовалось по «Программе аттестационных…»	Предоставлено Заявителем	Рег. номер документа
11	План контролируемой зоны	Приказ об определении границ контролируемой зоны	№ 349дсп от 16.03.2018 г.
12	Сертификаты соответствия требованиям по безопасности информации на программные и технические средства ИСПДн, используемые средства защиты	Сертификат соответствия на «Secret Net 7»	№ 2707 действителен до 07.09.2018 г.
13		Сертификат соответствия на СКЗИ «Программный комплекс С-Терра Клиент Версия 4.1»	№ СФ/114-3227 действителен до 15.11.2019 г.
14		Сертификат соответствия на средство антивирусной защиты «Kaspersky Endpoint Security 10 для Windows»	№ 3025 действителен до 25.11.2019 г.
15		Сертификат соответствия на Межсетевой экран « Программный комплекс С-Терра Клиент Версия 4.1»	№ СФ/114-3227 действителен до 15.11.2019 г.
16	Эксплуатационная документация	Инструкция администратору информационных систем персональных	б/н от 21.03.2018 г.
17		Инструкция пользователям информационных систем персональных	б/н от 21.03.2018 г.
18		Инструкция по эксплуатации СЗИ в информационных системах персональных	б/н от 21.03.2018 г.
19		Инструкция по организации антивирусной защиты в информационных системах персональных	б/н от 21.03.2018 г.
20		Инструкция по организации парольной защиты в информационных системах персональных	б/н от 21.03.2018 г.

Аттестационные испытания были проведены в следующем порядке:

- проанализированы и оценены представленные исходные данные и документация по защите информации на объекте информатизации;
- осуществлена проверка соответствия представленных исходных данных реальным условиям размещения, монтажа СВТ и эксплуатации СЗИ, рассмотрен технологический процесс обработки и хранения информации, определен состав и структура использованных для обработки информации технических и программных средств вычислительной техники;
- проверено состояние организации работ и выполнения организационно-технических требований по защите ПД, наличие организационно-распорядительной, проектной и эксплуатационной документации, ее соответствие требованиям государственной и отраслевой нормативной документации по безопасности информации, подготовки кадров и распределения ответственности за выполнение требований по обеспечению безопасности информации;
- проведены комплексные испытания ИСПДн на соответствие требованиям безопасности информации от НСД;
- подготовлена отчетная документация и настоящее заключение по результатам аттестационных испытаний.

4 РЕЗУЛЬТАТЫ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ

В результате проверки организации работ и готовности к функционированию ИСПДн на соответствие требованиям безопасности информации установлено:

4.1 Перечень представленных нормативных и организационно-распорядительных документов достаточен и их содержание соответствует требованиям стандартов и других нормативных документов по безопасности информации ФСТЭК России и иных органов государственного управления в пределах их компетенции.

4.2 Присвоение уровня защищенности информации, обрабатываемой в информационной системе проведено без нарушений требований руководящих документов и в соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Уровень защищенности информационной системы персональных данных – «4УЗ».

4.3 В организации произведен анализ угроз безопасности обрабатываемых персональных данных, модель угроз составлена без нарушений требований руководящих документов.

4.4 В организации приняты меры по ограничению доступа посторонних лиц к техническим средствам обработки защищаемой информации. Визуальный просмотр обрабатываемой на объекте информации посторонними лицами невозможен. Окна помещения, в которых расположен объект информатизации, оборудовано жалюзи. Помещение, в котором установлены ОТСС и хранятся машинные носители информации, оборудовано надежными замками, используются технические средства охраны и сигнализации. Допуск посторонних лиц в помещение ограничен и без контроля невозможен.

4.5 Допуск работников к персональным данным обеспечивается в рамках действующей в организации разрешительной системы и в соответствии с возложенными на персонал функциями.

4.6 На объекте имеются инструкции, на основании которых осуществляется работа пользователей, администраторов и обслуживающего персонала. Имеется эксплуатационная документация на используемые средства защиты информации.

4.7 Используемые средства защиты информации позволяют выполнить требования по обеспечению безопасности персональных данных.

4.8 Требования руководящих документов по защите информации от несанкционированного доступа к уровню защищенности информационных систем персональных данных «4УЗ» в части подсистем управления доступом, регистрации событий, обеспечения целостности и антивирусной защите выполнены.

4.9 Сертификаты соответствия на используемые средства защиты информации подтверждают возможность использования СЗИ в информационной системе персональных данных уровня защищенности «4УЗ».

5 ПРОТОКОЛ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, ПО НАПРАВЛЕНИЮ «ПРОВЕРКА ОБЪЕКТА НА СООТВЕТСТВИЕ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИМ ТРЕБОВАНИЯМ»

Общие положения

Аттестационные испытания ИСПДн проводились в соответствии с разделом 2 «Программы и методики проведения аттестационных испытаний…» (уч. № 3438дсп от 23.03.2018 г.) в следующем порядке: Состав основных технических средств и систем (ОТСС), системного и прикладного программного обеспечения, а также средств и систем защиты информации объекта информатизации приведен в Таблице 2.1, а также техническом паспорте на ИСПДн.

Результаты испытаний. Проверка достаточности представленных документов и соответствия их содержания требованиям по безопасности информации

Аттестационной комиссии были представлены исходные данные и документация на объект информатизации, приведенные в Таблице 3.1.

Заключение: *В предоставленных документах (см. Таблицу 3.1) содержатся все необходимые исходные данные об объекте информатизации. Дополнительных документов не требуется.*

Исследование технологического процесса обработки и хранения информации, анализ информационных потоков, определение состава использованных для обработки информации технических средств

5.3.1 При проведении исследования технологического процесса обработки информации на объекте информатизации, было определено, что:

объектами доступа ИСПДн являются:

а) ПЭВМ в целом;

б) машинные носители информации (в т.ч. НЖМД, флэшкарты, CD/DVD-диски);

в) коммуникационные порты системного блока (COM, USB, PS/2, DVI, RJ-45, MiniJack 3.5);

г) файлы, содержащие защищаемые сведения;

д) программное обеспечение (общесистемное и прикладное);

е) основные и вспомогательные технические средства;

ж) средства и системы защиты информации.

субъектами доступа в ИСПДн являются:

а) прикладное программное обеспечение, применяемое для создания и/или редактирования файлов;

б) администратор информационной безопасности, осуществляющий администрирование программно-аппаратного комплекса СЗИ от НСД, а также установку и настройку прикладного и системного программного обеспечения;

в) пользователь, работающий на ПЭВМ;

г) обслуживающий персонал, осуществляющий техническое обслуживание средств вычислительной техники;

5.3.2 Была проанализирована обобщенная технологическая схема ИСПДн с существующими и возможными информационными потоками, возможностями доступа к обрабатываемой и передаваемой информации.

5.3.3 Было проверено соответствие описания технологического процесса обработки и хранения защищаемой информации с реальной технологией обработки данных на объекте. Противоречий не обнаружено.

Заключение: *Описание технологического процесса обработки и хранения конфиденциальной информации соответствует реальной практике, принятой на рассматриваемом объекте информатизации.*

5.3.4 Были проверены предоставленные исходные данные на рассматриваемую автоматизированную систему, комплектность и характеристики применяемых средств и систем защиты информации. Проанализированы вероятные опасные факторы и угрозы, которые могут воздействовать на автоматизированную систему, рассмотрены потенциально возможные критические места автоматизированной системы, снижающие уровень защиты.

Заключение: *Анализ исходных данных по автоматизированной системе не выявил опасных факторов, угроз и критических мест в автоматизированной системе, снижающих уровень защищенности информации и характеристики средств защиты информации.*

Проверка правильности присвоения уровня защищенности объекта информатизации и классификации ИСПДн

В организации Общество с ограниченной ответственностью «Завод углеродных и композиционных материалов» обрабатываются персональные данные категории «Иные» сотрудников, третий тип актуальных угроз, объем обрабатываемых данных менее 100 000 субъектов персональных данных. С учётом вида и объема персональных данных, типа и технологического процесса обработки, ИСПДн присвоен уровень «4УЗ» с многопользовательский режимом обработки и различными правами доступа. Определённый и установленный уровень защищенности ИСПДн соответствуют друг другу.

Заключение: *Классификация проведена без нарушений требований руководящих документов ФСТЭК (Гостехкомиссии) России.*

Проверка уровня подготовки кадров и распределения ответственности между персоналом по следующим направлениям:

– на объекте информатизации принята и подтверждена соответствующими организационно-распорядительными документами разрешительная система доступа персонала к защищаемым ресурсам;

– пользователи, администраторы и обслуживающий персонал подтвердили знание эксплуатационной документации (в пределах выполнения своих производственных задач), уровень овладения ими технологии безопасной обработки информации соответствует требованиям, изложенным в эксплуатационной документации;

Заключение: *Уровень подготовки кадров и распределение ответственности персонала, разрешительная система доступа персонала к защищаемым ресурсам объекта информатизации, определяющая полномочия по доступу к защищаемой информации, а также процедура оформления их полномочий, соответствуют предъявляемым к ним требованиям.*

Проверка наличия сертификатов соответствия на технические средства и средства защиты информации

На используемые средства защиты информации были представлены сертификаты, указанные в таблице 3.1.

Сертификаты подтверждают возможность использования средств защиты в ИСПДн данного класса.

Заключение: *На используемые средства защиты информации предоставлены все необходимые сертификаты. Сертификаты соответствуют уровню защищенности ИСПДн.*

Проверка выполнения требований к помещениям, в которых производится обработка информации

Помещение оборудовано средствами пожарной и охранной сигнализации, доступ в помещение возможен только под присмотром сотрудников организации. Технические средства обработки защищаемой информации отдалены от границы контролируемой зоны. Просмотр информации с экранов мониторов, распечаток принтеров и с других устройств ввода-вывода информации из-за пределов контролируемой зоны исключён.

Заключение: *Требования руководящих документов по условиям размещения технических средств в помещениях выполняются.*

Выводы аттестационной комиссии

По результатам аттестационных испытаний комиссия считает, что:

5.8.1 Перечень представленных нормативных и организационно-распорядительных документов достаточен и их содержание соответствует требованиям стандартов и других нормативных документов по безопасности информации ФСТЭК России, ФСБ и иных органов государственного управления в пределах их компетенции.

5.8.2 Реализация требований инструкций и применение сертифицированных СЗИ от НСД обеспечивает выполнение установленных требований по защите информации при использовании технических и программных средств вычислительной техники.

5.8.3 Состав и структура программно-технических средств автоматизированной системы соответствует представленной документации.

5.8.4 Классификация автоматизированной системы проведена без нарушений требований руководящих документов ФСТЭК (Гостехкомиссии) России.

5.8.5 Помещение, в котором расположены ОТСС, отвечает требованиям руководящих документов, предъявляемым к рабочим помещениям, в которых устанавливаются СВТ для обработки информации с ограниченным доступом.

5.8.6 Допуск персонала к работе обеспечивается в рамках действующей в организации разрешительной системой и в соответствии с возложенными на персонал функциями.

5.8.7 Уровень подготовки персонала позволяет реализовать установленные для данного объекта информатизации требования по безопасности информации.

6 ПРОТОКОЛ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ ОБЪЕКТА ИНФОРМАТИЗАЦИИ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Общие положения

ИСПДн построена на базе основных технических средств и систем, системного и прикладного программного обеспечения, а также средств и систем защиты информации, состав которых приведен в Таблице 2.1, а также техническом паспорте на ИСПДн.

Результаты проведения проверки качества и эффективности функционирования системы защиты информации от несанкционированного доступа

При проведении проверки качества и эффективности функционирования системы защиты информации от несанкционированного доступа проверяющая сторона руководствовалась следующими руководящими и нормативно-методическими документами:

- Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности СВТ»;
- Постановление об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных (утв. Постановлением Правительства РФ от 01.11.2012 г № 1119);
- 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».

Анализ и оценка технологического процесса обработки информации

Проверка состояла:

- в анализе состояния реального технологического процесса обработки информации в ИСПДн;
- в выработке заключения о ее соответствии конструкторской (проектной), эксплуатационной и организационно-распорядительной документации на ИСПДн, предоставленной проверяющей стороной.

В рамках данного пункта проверки были проведены следующие мероприятия:

- анализ соответствия состава объектов и субъектов доступа, средств передачи и обработки информации исходным данным по функционированию ИСПДн, разрешительной системе доступа персонала к защищаемым ресурсам и соответствия реального технологического процесса обработки информации на средствах ИСПДн представленному описанию технологического процесса;
- определение опасных факторов и угроз, критических мест ИСПДн, снижающих уровень защиты; проверка наличия документов по разрешительной системе доступа персонала к защищаемой информации, хранящейся и (или) обрабатываемой в ИСПДн;
- проверка соответствия технологических инструкций пользователя и администратора защиты информации установленным требованиям.

В ходе проверки проверяемой стороной были представлены документы (см. Таблицу 3.1).

Анализ соответствия состава объектов и субъектов доступа, средств передачи и обработки информации исходным данным по технологии функционирования автоматизированной системы, разрешительной системе доступа персонала к защищаемым ресурсам

В процессе анализа были выполнены следующие операции:

- определен состав и режимы функционирования средств передачи и обработки информации, среды передачи информации;
- определены объекты и субъекты доступа, перечни штатных средств доступа к информации, средства защиты информации;
- проверено функционирование системы доступа персонала к защищаемым ресурсам.

Состав и функционирование средств передачи и обработки информации, среды передачи и обработки информации

На момент проведения проверки качества и эффективности функционирования системы защиты информации от несанкционированного доступа ИСПДн «Бухгалтерия» включает в себя одно автоматизированное рабочее место (АРМ), расположенное в Бухгалтерии под управлением операционной системы «Microsoft Windows 7 Enterprise Service Pack 1».

Внешними устройствами «Бухгалтерия» являются МФУ, подключенное к компьютеру по LAN интерфейсу, флешкарты. Рабочая станция подсоединена к локальной сети, являющейся внешней по отношению к ИСПДн. На рабочей станции установлен сертифицированный программный межсетевой экран. ЛВС соединена с сетями общего пользования через маршрутизатор.

ИСПДн «Бухгалтерия» является многопользовательской системой с разграничением пользователей.

Защищаемая информация хранится на жёстком диске АРМ. Сетевой доступ к данным не предоставляется. Технологическим процессом предусмотрен вывод документов на «твердую» копию.

К работе с персональными данными допускаются лишь сотрудники, указанные в утверждённом списке.

Носители информации (НЖМД, флэшкарты, CD/DVD-диски, бумажные носители) учитываются, выдаются, уничтожаются согласно установленному порядку, что отражается в специальных журналах.

Перечень объектов и субъектов доступа

Анализ технологического процесса показал, что объектами доступа являются:

- ОТСС, предназначенные для обработки и передачи ПД, приведенные в техническом паспорте;
- программные средства ИСПДн, предназначенные для обработки и передачи ПД;
- учтенные машинные носители информации (далее - МНИ): НЖМД, флэшкарты, CD/DVD-диски;
- все виды памяти ПЭВМ ИСПДн, в т.ч. оперативная память ПЭВМ, в которых может находиться защищаемая информация;
- база персональных данных специализированного программного обеспечения.

Субъектами доступа в ИСПДн являются пользователи и процессы, выполняемые от их имени, которые имеют возможность доступа к объектам в ИСПДн штатными средствами. Субъектам доступа присваиваются официальные полномочия на уровне подсистемы защиты информации.

В процессе анализа технологического процесса обработки информации в ИСПДн установлено, что все субъекты доступа идентифицируются по имени учетной записи и аутентифицируются по паролям средствами СЗИ от НСД «Secret Net 7».

Перечень штатных средств доступа к информации в автоматизированной системе

Проверялось наличие штатных средств доступа к информации в ИСПДн.

Доступ к информации обеспечивается системным программным обеспечением ОС, а также с помощью прикладного программного обеспечения, указанного в «Техническом паспорте», предоставляющего субъектам документированные возможности доступа к объектам.

Произведен анализ состава программного обеспечения на наличие потенциально опасных или запрещенных программных модулей.

Произведен расчет контрольных сумм исполняемых модулей (компонентов) системы защиты информации от несанкционированного доступа средствами программы фиксации и контроля исходного состояния программного комплекса «ФИКС» версии 2.0.1

(Сертификат ФСТЭК России № 913 от 28 мая 2004 года, действителен до 1 июня 2019 года. Знак соответствия: № А 267757. Регистрационный номер: ЦС50-467А267757).

Перечень средств защиты информации

Проверялся перечень имеющихся средств защиты информации в ИСПДн.

На АРМ ИСПДн установлены СЗИ от НСД «Secret Net 7», средство антивирусной защиты «Kaspersky Endpoint Security 10 для Windows», межсетевой экран «Программный комплекс С-Терра Клиент Версия 4.1», СКЗИ «Программный комплекс С-Терра Клиент Версия 4.1».

Согласно представленным документам, при обработке защищаемой информации дополнительно проводятся организационно-технические мероприятия, обеспечивающие требуемый режим конфиденциальности, а также целостность и сохранность персональных данных.

Проверка разрешительной системы доступа персонала к защищаемым ресурсам

Проверка заключалась в анализе организационно-распорядительной документации, устанавливающей разрешительную систему доступа персонала к защищаемым ресурсам ИСПДн. Анализ показал, что действующими факторами разрешительной системы являются:

- определение и документальное закрепление перечня сотрудников, допущенных к обработке конфиденциальной информации на данной ИСПДн.
- определение и документальной закрепление разрешительной системы доступа в матрице доступа.
- размещение АРМ в условиях ограниченного и контролируемого доступа;
- действия персонала (администратора защиты), имеющего доступ к автоматизированному рабочему месту, регламентированы специальными инструкциями;
- сопровождение и контроль функционирования ИСПДн осуществляется только администратором защиты ИСПДн.

Определение опасных факторов и угроз, критических мест автоматизированной системы, снижающих уровень защиты

В рамках данной проверки были выполнены следующие операции:

- проверен порядок организации охраны помещений, где установлены рабочие места ИСПДн;
- проверен порядок хранения в архивах копий программного обеспечения и конфигурационных данных;
- проверена настройка программных средств, посредством которых осуществляется доступ к объектам.

Анализ структуры ИСПДн и технологического процесса обработки информации показал, что в качестве основных факторов риска для ИСПДн может рассматриваться разглашение ПДн сотрудниками, допущенными к обработке ПДн.

Основными механизмами уменьшения факторов риска применительно к уязвимым местам ИСПДн, реализованными в ИСПДн на момент проведения проверки качества и эффективности функционирования системы защиты информации от НСД, является наличие необходимой организационно-распорядительной документации.

Вывод: Используемые средства защиты информации и организационно-технические меры позволяют избежать проявления выявленных угроз безопасности информации.

Проверка соответствия технологических инструкций пользователя и администратора защиты информации установленным требованиям

Была проведена проверка оформленных разрешений на допуск персонала к различной защищаемой информации и соответствия технологических инструкций пользователям и администратору защиты установленным требованиям.

В рамках данной проверки были выполнены следующие операции:

- проверено наличие утвержденных разрешений на доступ персонала к защищаемой информации (ПДн);
- проверено наличие и содержание технологической инструкции для пользователей ИСПДн;
- проверено наличие и содержание технологических инструкций для администратора защиты ИСПДн.

Установлено, что разрешения на доступ персонала к информации в ИСПДн, технологические инструкции пользователям и администратору защиты соответствуют требованиям нормативных документов по безопасности информации.

Вывод по разделу 6.3: Состав объектов и субъектов доступа, средств передачи и обработки информации в ИСПДн соответствует представленной документации, исходным данным по технологии функционирования ИСПДн, разрешительной системе доступа персонала к защищаемым ресурсам. В ИСПДн выполняются требования РД по документальному закреплению разрешительной системы доступа. Защитные механизмы уменьшают выявленные факторы и угрозы безопасности информации. В ИСПДн определены технологические инструкции пользователям и администратору.

Выбор инструментальных средств и методики испытаний.

По результатам анализа технологического процесса в соответствии с «Программой и методикой проведения испытаний…» решено проводить испытания подсистем управления доступом, регистрации и учёта, контроля целостности и антивирусной защиты на соответствие требованиям руководящих документов по защите информации. При проведении испытаний решено пользоваться специальными средствами проверки, определёнными в таблице 1.2 «Программы и методики…», а также проверкой реализованных функций средств защиты, просмотром журналов безопасности и другими методами, определёнными методикой испытаний.

6.4.1 Идентификация и аутентификация субъектов доступа и объектов доступа

Идентификация субъектов доступа осуществляется по имени учетной записи в системе. Аутентификация субъектов производится посредством пароля условно-постоянного действия не менее шести буквенно-цифровых символов. Идентификаторы для тестовых пользователей выбирались произвольно.

Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов осуществляется средствами ОС и СЗИ от НСД «Secret Net 7».

Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации предусмотрено в эксплуатационных документах Общества с ограниченной ответственностью «Завод углеродных и композитных материалов» на ИСПДн, в частности инструкциями пользователям ИСПДн и осуществляется средствами ОС и СЗИ от НСД «Secret Net 7».

Защита обратной связи при вводе аутентификационной информации осуществляется СЗИ от НСД «Secret Net 7».

Вывод: Идентификация и аутентификация субъектов доступа осуществляется.

Вывод: Подсистема управления доступом в АС, обеспечиваемая СЗИ в соответствии с принятой разрешительной системой и матрицей доступа, соответствует требованиям РД к ИСПДн уровня защищенности «4УЗ».

6.4.2 Проверка управления доступом субъектов доступа к объектам доступа в соответствии с матрицей доступа.

Проверялась правильность предоставления доступа в соответствии с установленными правами субъектов по отношению к конкретным объектам в соответствии с матрицей доступа.

Управление учетными записями пользователей, реализация правил разграничения доступа, управление информационными потоками между устройствами, сегментами информационной системы осуществляется средствами ОС и СЗИ от НСД «Secret Net 7».

ИСПДн построена на базе одной операционной системы «Windows 7 Professional», обмен информацией между различными ОС не ведется.

Права администратора безопасности и пользователей по доступу к информационным ресурсам ИСПДн отличаются. Разграничение доступа производятся на основании настроек операционной системы, которые производятся для пары «объект-субъект», где в качестве объекта выступает либо том, либо директория, либо конечный файл, а в качестве субъекта - учетные записи пользователей, а также пользовательские группы.

Всем лицам, имеющим доступ к ИСПДн назначены минимально необходимые права и привилегии.

Число неуспешных попыток входа в информационную систему ограниченно СЗИ от НСД «Secret Net 7» и установлено равным 5.

После установленного времени бездействия пользователя (15 минут) или по его запросу происходит блокирование сеанса доступа в информационную систему.

Действия пользователей в системе до идентификации и аутентификации запрещены.

Защищенный удаленный доступ субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети осуществляется средствами СЗИ от НСД «Secret Net 7» (VPN, и т.д.).

Управление взаимодействием с информационными системами сторонних организаций и внешними информационными системами осуществляется средствами СЗИ от НСД «Secret Net 7», межсетевым экраном «Программный комплекс С-Терра Клиент Версия 4.1». Дополнительный контроль осуществляется средством обнаружения вторжений.

Удаленный доступ к ИСПДн не предоставляется. Технологии беспроводного доступа и мобильные технические средства в ИСПДн не используются. Взаимодействием с информационными системами сторонних организаций не ведется.

Проверка проводилась с использованием программы контроля полномочий доступа к информационным ресурсам «РЕВИЗОР-2 XP» (Сертификат ФСТЭК России № 990 от 08 февраля 2005 года, действителен до 08 февраля 2020 года. Регистрационный номер программы: ЦС-50-0427А268720). Данные для контроля формировались средством создания модели системы доступа «Ревизор-1 XP» (Сертификат ФСТЭК России № 989 от 08 февраля 2005 года, действителен до 08 февраля 2020 года. Регистрационный номер: ЦС50-0427А296220).

При попытке доступа пользователя к запрещенным настройкам, система прекращает выполнение запроса и выдает предупреждающее сообщение.

Вывод: Контроль доступа к защищаемым ресурсам производится в соответствии с матрицей доступа средствами операционной системы и СЗИ, что соответствует требованиям РД к ИСПДн уровня защищенности «4УЗ».

6.4.3 Ограничение программной среды

Регистрации запуска/завершения программ и процессов (заданий, задач) осуществляется при помощи средств операционной системы и СЗИ.

Проверка осуществлялась путем запуска/завершения любой доступной программы, и просмотра журнала безопасности на наличие соответствующего события. Проверялось наличие параметров регистрации, требуемых РД. В параметрах регистрации указывается путь к выполняемому файлу, используемые библиотеки, дата и время запуска, идентификатор пользователя, результат запуска.

Вывод: Средства операционной системы и СЗИ в полной мере реализуют требуемые РД параметры регистрации указанных событий.

6.4.4 Защита машинных носителей информации, на которых хранятся и обрабатываются персональные данные

Охрана здания, в котором размещается ИСПДн, осуществляется постоянно с помощью технических средств охраны и организационных мер, что исключает неконтролируемое пребывание посторонних лиц в помещения в которых обрабатываются и хранятся персональные данные. Использование не учтенных съемных носителей информации контролируется СЗИ.

Учет машинных носителей персональных данных ведется в журнале «Secret Net 7».

Вывод: В ИСПДн установлено СЗИ предотвращающее использование неучтенных съемных носителей информации, а так же предотвращен неконтролируемый доступ в помещения в которых находятся машинные носители информации, что соответствует требованиям РД к ИСПДн уровня защищенности «4УЗ».

6.4.5 Регистрация событий безопасности

Регистрация запуска/завершения программ и процессов (заданий, задач) осуществляется при помощи средств операционной системы и СЗИ.

Проверка осуществлялась путем запуска/завершения любой доступной программы, и просмотра журнала безопасности на наличие соответствующего события. Проверялось наличие параметров регистрации, требуемых РД. В параметрах регистрации указывается путь к выполняемому файлу, используемые библиотеки, дата и время запуска, идентификатор пользователя, результат запуска.

События безопасности, подлежащие регистрации, и сроки их хранения определены настройками ОС и СЗИ от НСД «Secret Net 7». В течение установленного времени средствами ОС и СЗИ от НСД «Secret Net 7» ведется сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения.

Мониторинг результатов регистрации событий безопасности и реагирование на них осуществляется администратором безопасности в соответствие с должностными и функциональными инструкциями.

Средства операционной системы и СЗИ в полной мере реализуют требуемые РД параметры регистрации указанных событий.

Проверка осуществлялась путем запуска на АРМ прикладных программ для получения доступа к защищаемым ресурсам. Доступ к ресурсу устанавливается в соответствии с разрешениями и текущим уровнем доступа исполняемого процесса.

Средства операционной системы и СЗИ осуществляют регистрацию попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам в объеме, требуемом РД.

Проверка наличия регистрации событий в журнале СЗИ.

Вывод: Параметры регистрации запуска/завершения программ и процессов удовлетворяют требованиям РД к ИСПДн уровня защищенности «4УЗ». Средствами операционной системы и СЗИ осуществляется полная регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам и данным, что удовлетворяет требованиям РД к ИСПДн уровня защищенности «4УЗ». Осуществляется регистрация событий безопасности в журнале СЗИ.

6.4.6 Антивирусная защита

В качестве антивирусной защиты на АРМ АС установлена лицензионная копия сертифицированного антивирусного программного обеспечения «Kaspersky Endpoint Security 10 для Windows». Администратор ИСПДн производит регулярное обновление базы данных признаков вредоносных компьютерных программ.

Условия, порядок и правила использования антивирусного программного обеспечения определены в «Инструкции по организации антивирусной защиты». Ответственность за организацию и проведения антивирусного контроля возложена на администратора информационной системы.

Вывод: Условия эксплуатации и обновления антивирусного программного обеспечения соответствуют требованиям РД к ИСПДн уровня защищенности «4УЗ».

6.4.7 Контроль защищенности персональных данных

Выявление уязвимостей информационной системы и их оперативное устранение ведется администратором информационной безопасности, назначенным распоряжением «Об организации работ по обеспечению безопасности персональных данных в ООО Завод углеродных и композиционных материалов » № 2 от 05.09.2017 г. Администратор информационной безопасности осуществляет проверку установки обновлений ПО и программных средств СЗИ, осуществляет контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и СЗИ, контроль состава технических средств, ПО и СЗИ, контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализация правил разграничения доступа, полномочий пользователя в информационной системе.

Была проверена парольная политика системы, а так же наличие обновлений безопасности операционной системы.

В ходе проверки были устранены выявленные уязвимости, осуществлен контроль установки обновлений, правильность настройки программ, состав технических средств, ПО и СЗИ, а так же проверена правильность используемых паролей

Вывод: Контроль защищенности системы соответствуют требованиям РД к ИСПДн уровня защищенности «4УЗ».

6.4.8 Обеспечение целостности информационной системы персональных данных

Целостность программных средств системы защиты информации обеспечивается проверкой контрольных сумм компонентов системы защиты при загрузке системы.

Целостность программной среды обеспечивается отсутствием средств модификации объектного кода программ на рабочих станциях ИСПДн.

Вывод: В ИСПДн обеспечивается целостности программной среды, включая программное обеспечение средств защиты информации в соответствии с требованиями РД к ИСПДн уровня защищенности «4УЗ».

6.4.9 Обеспечение доступности персональных данных

Была выполнена проверка резервного копирования и возможности восстановления данных из резервных копий. Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных выполняется согласно Инструкции по резервному копированию и восстановлению ресурсов.

Вывод: Резервное копирование выполняется, а так же существует возможность восстановление ПДн с резервных носителей.

6.4.10 Защита среды виртуализации

Средства виртуализации в ИСПДн не используются.

Вывод: Защита среды виртуализации соответствует требованиям РД для ИСПДн уровня защищенности «4УЗ».

6.4.11 Защита технических средств

В здании, в котором расположены технические средства ИСПДн, определён пропускной режим. Доступ посторонних лиц возможен только при предъявлении документа, удостоверяющего личность. Охрана здания, в котором размещается ИСПДн, осуществляется постоянно с помощью технических средств охраны и организационных мер, что исключает неконтролируемое пребывание посторонних лиц. Устройства вывода информации, расположены так, что исключается их несанкционированный просмотр. Окно занавешено жалюзи.

Вывод: В ИСПДн осуществляется физическая охрана средств вычислительной техники, размещение устройств вывода исключает несанкционированный просмотр информации, что соответствует требованиям РД к ИСПДн «4УЗ» уровня защищенности.

6.4.12 Защита информационной системы, ее средств, систем связи и передачи данных

Защиты персональных данных 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 осуществляется средствами СЗИ от НСД Secret Net 7 и межсетевым экраном Программный комплекс С-Терра Клиент Версия 4.1.

Вывод: В ИСПДн используются СЗИ, которые соответствует требованиям РД к ИСПДн 4УЗ уровня защищенности.

6.4.13 Выявление инцидентов, которые могут привести к сбоям или нарушению функционирования информационной системы и к возникновению угроз безопасности персональных данных, и реагирование на них

Приняты организационно-распорядительные документы, определяющие лиц, ответственных за выявление инцидентов и реагирование на них. Ведется проверка обнаружения, идентификации и регистрации инцидентов. Осуществляется своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами. Ведется анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий. Принимаются меры по устранению инцидентов и предотвращению их повторного возникновения, в частности обновление баз антивирусного ПО.

Вывод: В ходе проверки были определены ответственные, была проверена регистрация инцидентов и меры по устранению возникших инцидентов. Принятые меры соответствуют требованиям РД к ИСПДн уровня защищенности «4УЗ».

6.4.14 Управление конфигурацией информационной системы и системы защиты персональных данных

Вносить изменения в конфигурацию информационной системы и СЗИ может только администратор. Список работников, имеющих соответствующие права утвержден в Разрешительной системе доступа № 06-33/54дсп от 21.04.2018. Изменения конфигурации информационной системы и СЗИ выполняются только администраторами безопасности и согласуются с ответственным по обеспечению безопасности конфиденциальных данных.

Была произведена проверка документов, регистрирующих изменение в конфигурации информационной системы и системы защиты персональных данных.

Вывод: Меры управления конфигурацией информационной системы и системы защиты персональных данных соответствуют требованиям для уровня защищенности «4УЗ».

6.5 Выводы по результатам проверки качества и эффективности функционирования системы защиты информации от несанкционированного доступа

Результаты проведенных проверок показали, что автоматизированная система объекта информатизации информационная система персональных данных «Бухгалтерия», по совокупности используемых настроек СЗИ и принятых организационных мер **соответствует** требованиям Приказа ФСТЭК от 18 февраля 2013 г. №21 «О составе и содержании организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», предъявляемым **к ИСПДн уровня защищенности «4УЗ»**.

ЗАКЛЮЧЕНИЕ

Учитывая вышеизложенное, комиссия считает, что реализованные средства и меры защиты информации на объекте информатизации информационной системе персональных данных «Бухгалтерия», размещенном по адресу: г. Челябинск, Челябинский электродный завод, 5 этаж, Бухгалтерия, достаточны и соответствуют требованиям действующих нормативных документов по безопасности информации, предъявляемых к информационным системам персональных данных уровня защищенности «**4**».

Комиссия считает возможным выдать на аттестуемый объект информатизации «Аттестат соответствия…» на право обработки персональных данных категории «иные» в соответствии с установленным уровнем защищенности сроком на 3 года.

Председатель комиссии _____ К.С. Рыжов

Члены комиссии _____ А.С. Жаворонкин

_____ А.Ф. Морар

ПРИЛОЖЕНИЕ У

АКЦИОНЕРНОЕ ОБЩЕСТВО
ГРАНИТ ИНФОРМ
454006, г. Челябинск, ул. Красноармейская, 55
тел (351) 218 28 28, эл. почта: info@g-inform.ru

УТВЕРЖДАЮ

Руководитель органа по аттестации объектов информатизации
АО «Гранит Информ»

_____ Н.В. Узбеков

«_____»_____ 2018 г.

АТТЕСТАТ СООТВЕТСТВИЯ

№ АС/ДСП/34/18

на объект информатизации

информационную систему персональных данных

««Бухгалтерия»

Общества с ограниченной ответственностью «Завод углеродных и композитных материалов»

ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Выдан: 23 апреля 2018 г.

Действителен до: 22 апреля 2021 г.

2018 г.

1 Настоящим АТТЕСТАТОМ удостоверяется, что объект информатизации информационная система персональных данных «Бухгалтерия» Общества с ограниченной ответственностью «Завод углеродных и композитных материалов», расположенный в кабинет бухгалтерии, по адресу: г. Челябинск, Челябинский электродный завод, 5 этаж, кабинет бухгалтерии, соответствует требованиям безопасности информации, предъявляемым к объектам информатизации уровня защищенности «4УЗ».

2 Состав комплекса технических и программных средств, и продукции, используемой в целях защиты информации, а также схема их размещения на объекте и относительно границ контролируемой зоны, а также перечень средств защиты приведены в приложении к аттестату.

3 Организационная структура, нормативное и методическое обеспечение и техническая оснащенность Общества с ограниченной ответственностью «Завод углеродных и композитных материалов», обеспечивают поддержание уровня защищенности объекта информатизации в процессе эксплуатации в соответствии с установленными требованиями.

4 Аттестация «Бухгалтерия» выполнена в соответствии с программой и методикой испытаний, утвержденными руководителем органа по аттестации уч. № 3434дсп от 23.03.2018 г.

5 С учетом результатов аттестационных испытаний на «Бухгалтерия» разрешается обработка информации уровня защищенности не выше «4УЗ».

6 При эксплуатации ОИ запрещается:

- вносить изменения в комплектность ОИ, которые могут снизить уровень защищенности информации;
- проводить обработку защищаемой информации без выполнения всех мероприятий по защите информации;
- подключать к основным техническим средствам нештатные блоки и устройства;
- вносить изменения в состав, конструкцию, конфигурацию, размещение средств вычислительной техники;
- допускать к обработке защищаемой информации лиц, не оформленных в установленном порядке;
- производить копирование защищаемой информации на неучтенные носители информации, в том числе для временного хранения информации;
- обрабатывать на ПЭВМ защищаемую информацию при обнаружении каких-либо неисправностей;
- нарушать требования предписаний на эксплуатацию оборудования;
- заменять размещенные технические средства, изменять их комплектацию.

7 Контроль за эффективностью реализованных мер и продукцией, используемой в целях защиты информации, возлагается на ответственного за организацию обработки персональных данных.

8 Результаты испытаний «Бухгалтерия» приведены в заключении по результатам аттестационных испытаний уч. № 23.03.2018 от 3436дсп г.

9 Аттестат соответствия выдан на три года, в течение которых должна быть обеспечена неизменность условий функционирования «Бухгалтерия» и технологии обработки защищаемой информации, могущих повлиять на характеристики, указанные в п. 10.

10 Перечень характеристик, об изменениях которых требуется обязательно извещать орган по аттестации:

- состав и условия размещения технических средств и систем;
- состав и комплектность продукции, используемой в целях защиты информации, схема ее монтажа, параметры установки и настройки, способствующие снижению уровня защищенности объекта информатизации;
- характеристики систем (электропитания, заземления, сигнализации) обеспечения эксплуатации объекта информатизации.

Руководитель аттестационной комиссии
Заместитель генерального директора
АО «Гранит Информ» _____ К.С. Рыжов

_____»_____ 2018 г.

Приложение
К аттестату соответствия
№ АС/ДСП/34/18 от 23.04.2018 г.

Таблица 1 – Состав технических средств и систем объекта информатизации

№	Наименование и модель технических средств и систем объекта информатизации	Заводской номер
ОТСС		
1	Системный блок HP PRO 3500	RUA31706ZG
2	НЖМД ST500DM002-1BD142	Z3TEDYW1
3	Монитор HP 2011x	CNC128RQ3K
4	Клавиатура HP PR1101U	BAUWF11RZ1I911
5	Мышь Genius NetScroll 100X	X75891203592
6	Принтер Ricoh SP 3510SF/Aficio SP 3510SF	T333Q201268
7	Флешкарта Smartbuy 4Gb	90005A612A3BF021
8	Флешкарта Kingmax PI-03G2 8Gb	3HAC0381400000352
9	ИБП APC Back-UPS CS 500	4B1137P05147
ВТСС		
10	Датчик разбития стекла С2000-СТ	б/н
11	Датчик охранный объемный ИО 40910-8	б/н
12	Датчик пожарный Bolid ИП-212-34А	б/н
13	Телефон Panasonic KX-TS2570RU	8FAKC017337
14	Телефон Panasonic KX-TS2382RU	4AAKA038007
15	Телефон Panasonic KX-TS2351RU	7CAKB088004
16	Шредер HAMA	00050175
17	Кондиционер Hitachi	10301007
18	Обогреватель Polaris PRE S 0715 H	б/н
19	Терминал сбора данных Honeywell ScanPal 5100B0	1409630431
20	База синхронизации Honeywell 5100 Homebase	1415630045
21	Системный блок HP PRO 3500	RUA31706Z7
22	Монитор HP W2072a	CNC307PMN4

Таблица 2 – Перечень программных средств объекта информатизации

№	Наименование ПО	Версия
1	7-Zip	9.20.00.0
2	ABBYY FineReader 12 Corporate	12.1.609
3	Adobe Acrobat Reader DC	15.023.20053
4	Microsoft Office Professional Plus 2016	16.0.4266.1001
5	КОМПАС-3D Viewer	16.1
6	КриптоПро CSP	3.6.7777

Таблица 3 – Состав продукции, используемой в целях защиты информации объекта информатизации

№	Наименование	Заводской номер	Данные о сертификате, знаке соответствия (ЗС)
1	СЗИ от НСД «Secret Net 7»	GL83EB81, Л 643287	№ 2707 от 07.09.2012 г.
2	МЭ «Программный комплекс С-Терра Клиент Версия 4.1»	106096, К 169207	№ 3371 от 27.03.2015 г., № СФ/515-2659 от 20.07.2015 г.
3	СКЗИ «Программный комплекс С-Терра Клиент Версия 4.1»	106096, К 169207	№ 3371 от 27.03.2015 г., № СФ/114-2513 от 01.12.2014 г.
4	САВЗ «Kaspersky Endpoint Security 10 для Windows»	СМП8069-8854, Л 874356	№ 3025 от 25.11.2013 г.

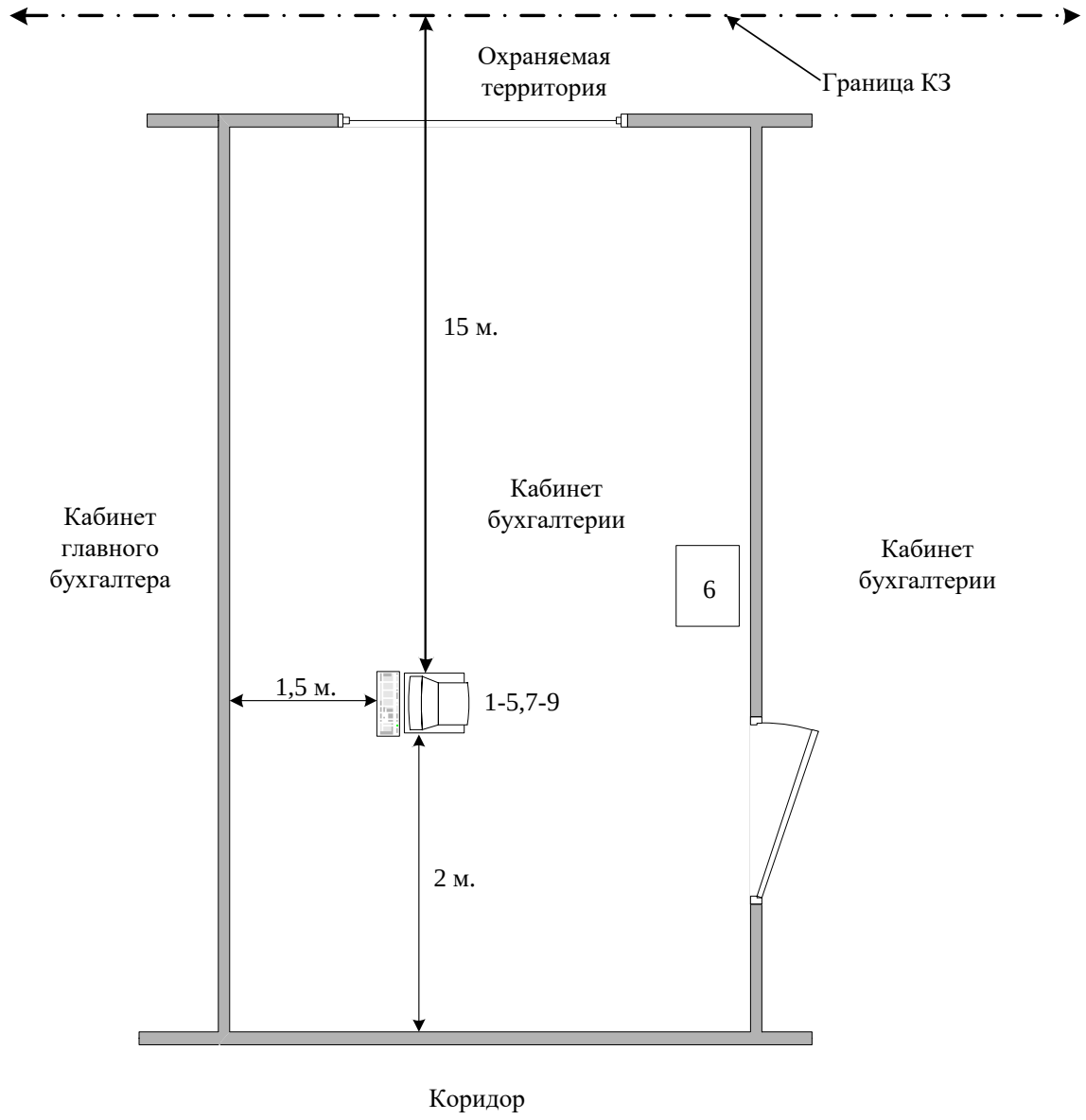

Рисунок 1 – Размещение ОТСС «Бухгалтерия» относительно границ контролируемой зоны

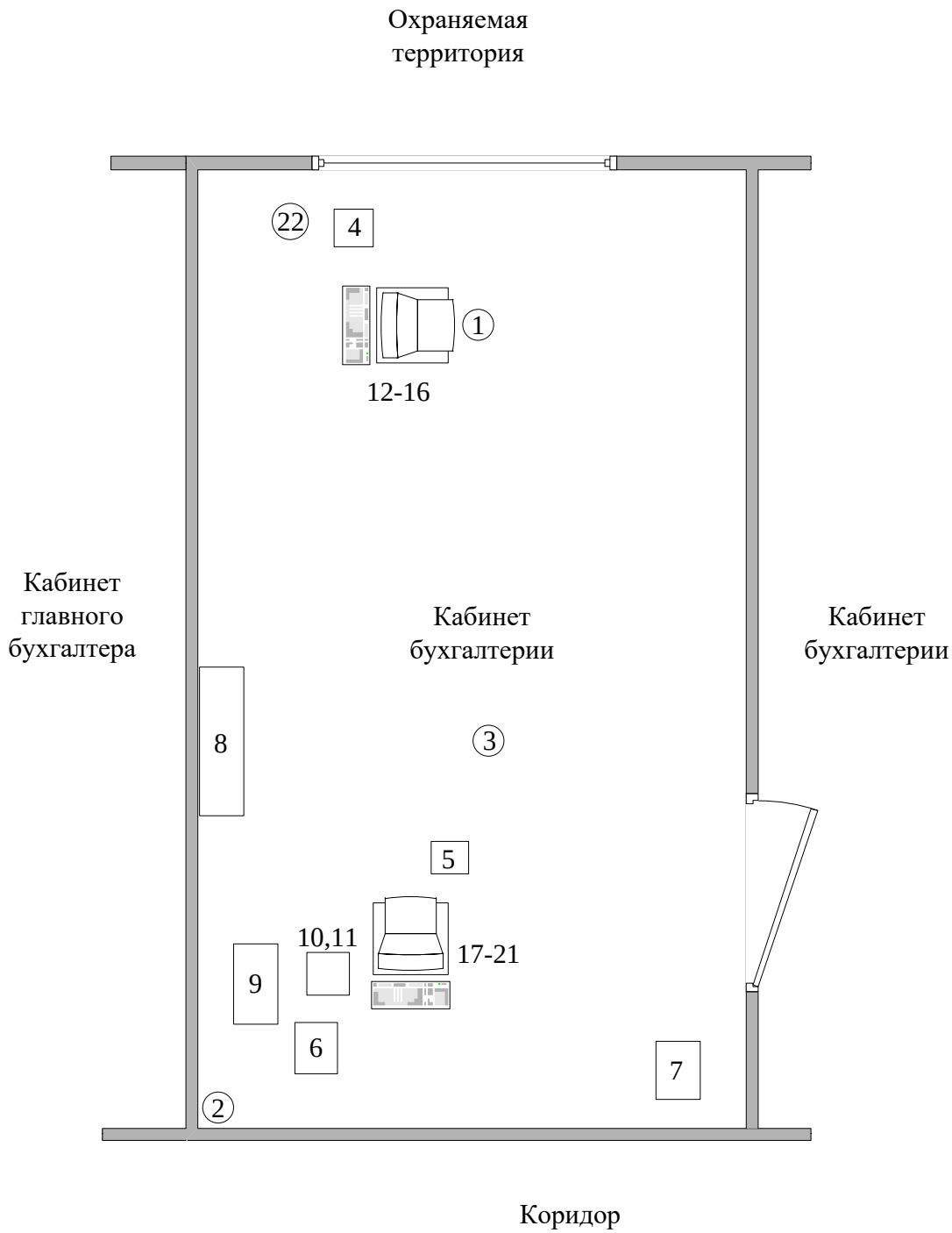

Рисунок 2 – Размещение ВТСС «Бухгалтерия»

Отметки органов контроля: