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, инженер-программист
управления информационных
технологий ФГУП «ПО «Маяк»»
_____ Н.Г. Ведюшкин
_____ 2018 г.

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

Аттестация информационной системы персональных данных в «Управлении информационными технологиями» государственного предприятия

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ – 10.05.03.2018.272.ПЗ ВКР

Консультанты

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

Руководитель проекта,
н.с. НОЦ «Информационная
безопасность» ВШ ЭКН
_____ А.Е. Баринов
_____ 2018 г.

Автор проекта,
студент группы КЭ-530
_____ Д.С. Силантьев
_____ 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
Силантьева Дмитрия Сергеевича

Группа *КЭ-530*

1 Тема работы

Аттестация информационной системы персональных данных в «Управлении информационными технологиями» государственного предприятия

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

2 Срок сдачи студентом законченной работы _____

3 Исходные данные к работе

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

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

1. Этап обследования объекта информатизации
2. Этап анализа технической документации
3. Этап аттестационных испытаний объекта информатизации
4. Безопасность жизнедеятельности

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

Презентация «Аттестация информационной системы персональных данных в «Управлении информационных технологий» государственного предприятия» в формате PowerPoint 2013 (pptx).

Количество слайдов -

Всего ___ листов

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

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

7 Дата выдачи задания _____

Руководитель_____ Е.А. Баринов

Задание принял к исполнению _____ Д.С. Силантьев

КАЛЕНДАРНЫЙ ПЛАН

Наименование этапов выпускной квалификационной работы (проекта)	**Срок выполнения этапов работы**	**Отметки о выполнении руководителя**
Введение		
1 Этап обследования объекта информатизации		
2 Анализ 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 _____ Е.А. Баринов

Студент _____ Д.С. Силантьев

АННОТАЦИЯ

Силантьев Д. С. Аттестация системы защиты информационной системы персональных данных в «Управлении информационных технологий» государственного предприятия – Челябинск: ЮУрГУ, КЭ-530, 159 с., 6 ил., 25 табл., библ. список – 15 наим., 13 прил.

Выпускная квалификационная работа выполнена с целью подготовки к аттестации системы защиты информационной системы персональных данных в «Управлении информационных технологий» на государственном предприятии «ПО «Маяк»». Работа состоит из четырех глав.

В первой главе проведен анализ информационной системы «ПО «Маяк»», в результате которого был разработан паспорт предприятия, выявлены объекты защиты, разработана модель угроз и уязвимостей, произведён расчёт рисков для выявленных объектов защиты.

Во второй главе разработан документ «Программа и методики проведения аттестационных испытаний», который сделан на основании анализа выявленных угроз, уязвимостей и возможных методов по их устранению.

В третьей главе проведены аттестационные испытания объекта информатизации.

В четвёртой главе проведен анализ потенциально опасных и вредных производственных факторов, на основе которых, выработаны рекомендации для работы организации.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Согласно ст.19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

В соответствии с требованиями законодательства необходимо разработать комплект организационно-распорядительной документации, соответствующий нормативно-правовым актам РФ в области обеспечения защиты персональных данных и провести оценку защищенности объектов информатизации по требованиям безопасности информации.

Документацию необходимо разработать 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» (далее по тексту – Приказ № 21).

Актуальность данной работы обоснована требованием законодательства.

Объектом выпускной квалификационной работы является «Информационная система персональных данных клиент-банка», находящаяся в управлении информационных технологий государственного предприятия.

Целью данной работы является аттестация по требованиям безопасности информации «Информационной системы персональных данных клиент-банка» в управлении информационных технологий государственного предприятия.

Для реализации поставленной цели необходимо:

– проанализировать исходные данные по аттестуемому объекту информатизации;

– предварительно ознакомиться с объектом информатизации;

– провести экспертное обследование объекта информатизации;

– разработать документ «Программа и методики проведения аттестационных испытаний» необходимый для проведения аттестационных испытаний по требованиям информационной безопасности информации;

– провести испытание отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальных средств проверки;

– провести комплексные аттестационные испытания объекта информатизации в реальных условиях эксплуатации;

– оформить протоколы аттестационных испытаний объекта информатизации на соответствие требованиям по защите информации от несанкционированного доступа и организационным требованиям по защите информации и, на основании их, выпустить заключение по результатам аттестационных испытаний.

СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ.

ВТСС	–	вспомогательные технические средства и системы;
ИС	–	информационная система;
ИСПДн	–	информационная система, предназначенная для обработки персональных данных;
ИСПДн КБ	–	«Информационная система персональных данных клиент-банка»;
КЗ	–	контролируемая зона;
ОИ	–	объект информатизации;
ОС	–	операционная система;
ОТСС	–	основные технические средства и системы;
ПДн	–	персональные данные;
ПК	–	персональный компьютер;
ПО	–	программное обеспечение;
ПЭВМ	–	персональная электронно-вычислительная машина;
ПЭМИН	–	побочные электромагнитные излучения и наводки;
САЗ	–	средства антивирусной защиты;
СВТ	–	средства вычислительной техники;
СЗИ	–	система защиты информации;
СЗИ НСД	–	средства защиты информации от несанкционированного доступа;
СБГП	–	служба безопасности государственного предприятия;
ТСО	–	технические средства охраны;
УИТ	–	управление информационных технологий;
ФСТЭК	–	Федеральная служба по техническому и экспортному контролю.

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

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

Критичность ресурса – степень значимости ресурса для информационной системы, т.е. как сильно повлияет реализация угроз информационной безопасности на работу информационной системы.

Аттестация – комплекс организационно-технических мероприятий, в результате которых подтверждается, что объект информатизации соответствует требованиям стандартов или иных нормативных документов по безопасности информации.

Объект информатизации – совокупность информационных ресурсов, средств и систем информатизации, используемых в соответствии с заданной информационной технологией, и систем связей вместе с помещениями, в которых они установлены.

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

1.ЭТАП ОБСЛЕДОВАНИЯ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

1.1. Общие сведения

Полное наименование информационной системы: «Информационная система персональных данных клиент-банка».

Сокращенное наименование: «ИСПДн КБ».

Заказчик – УИТ.

Исполнители - служба безопасности государственного предприятия.

Целью обработки ПДн в «ИСПДн КБ» является отправка зарплатных реестров в банки.

Обработку ПДн осуществляют работники УИТ.

Перечень действий с ПДн:

– получение зарплатных реестров;

– отправка зарплатных реестров в банки.

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.

В соответствии с пунктом 6 Приказа № 21, 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 Приказом № 21, форма оценки эффективности, а также форма и содержание документов, разрабатываемых по результатам оценки, не установлены.

Таким образом, решение по форме оценки эффективности и содержанию 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.

Для проведения аттестационных испытаний был предоставлен следующий комплект документов:

– техническое задание (Приложение А);

– описание технологического процесса обработки информации объекта информатизации УИТ государственного предприятия (Приложение Б);

– акт классификации ИСПДн (Приложение В);

– технический паспорт (Приложение Г);

– частная модель угроз и требования к системе защиты (Приложение Д);

– технологическая инструкция администратора ИБ (Приложение Е);

– технологическая инструкция по обеспечению защиты при работе в информационных системах, обрабатывающих конфиденциальную информацию (Приложение Ж);

– технологическая инструкция для технического обслуживающего персонала (Приложение З);

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».

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

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

1.2. Анализ технического задания ИСПДн КБ

Для аттестации системы защиты ИСПДн КБ был проведен анализ технического задания на создание ИСПДн КБ в управлении информационных технологий государственного предприятия. (Приложение А)

Техническое задание представляет собой документ, отражающий основные требования к разработке и внедрению системы защиты информации в «Информационной системе персональных данных клиент-банка».

В документе представлены требования по организационным мерам обеспечения безопасности информации, программно-техническим средствам защиты информации, к комплексу технических средств, к технической защите и технологическому процессу обработки информации.

Данная ИС находится в пределах контролируемой зоны. Границами контролируемой зоны являются стены здания (приказ о границах контролируемой зоны от 09.03.2018 № 146/279-А).

Обработка персональных данных субъектов ИСПДн КБ производится на основании ст. 6 ФЗ от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

ПДн используются для передачи платежных документов и зарплатных реестров в банки.

На основании исходных данных орган по аттестации принял решение о проведении аттестационных испытаний объекта информатизации ИСПДн КБ.

1.3. Обследование ИСПДн КБ

1.3.1. Характеристика информационной системы

«ИСПДн КБ» состоит из ПЭВМ, подключенной при помощи коммутационного оборудования в сеть Интернет, обрабатывающей ПДн.

Режим обработки персональных данных в системе – многопользовательский.

Целью данной задачи является отправка зарплатных реестров в банки.

По разграничению прав доступа пользователей «ИСПДн КБ» относится к системам с разграничением прав доступа.

Пользователи системы имеют равные права доступа к информации, обрабатываемой в задаче «Информационная система персональных данных клиент-банка»

В задаче обрабатывается информация следующего содержания: фамилия, имя, отчество, дата рождения, пол, место жительства, место работы и должность и прочие.

1.3.2. Характеристика комплекса технических средств

Комплекс технических средств состоит из ПЭВМ, подключенного при помощи коммутационного оборудования в сеть Интернет и принтера.

Для ведения резервных копий, а также обновления ПО и антивирусных баз используются флэш-накопители.

Отчуждаемый флэш-накопитель, предназначенный для обновления ПО и антивирусных баз, не предназначен для хранения ПДн и используется только администратором ИБ.

Флэш-накопители для хранения резервных копий хранятся в сейфе.

В комплекс ВТСС входят телефонные аппараты, датчики ТСО, датчики пожарной сигнализации, линии и радиоприемники радиотрансляционной сети, линии электропитания, линии связи, металлические конструкции и коммуникации.

1.3.3. Характеристика программного обеспечения

В комплекс программных средств, установленных на ЭВМ входят:

– ОС Microsoft Windows 7 Professional SP1 Russian;

– специальное ПО «Клиент-банк»;

– антивирусное ПО Kaspersky Endpoint Security;

– Microsoft Office 2007;

– Total Commander.

1.3.4. Режимы работы ИСПДн КБ

В ИСПДн КБ организован многопользовательский режим работы. Пользователи имеют равные права доступа к обрабатываемой информации.

Пользователи ИСПДн КБ входят в локальную группу «Пользователи». В данном режиме доступны следующие ресурсы:

- принтер;
- программные и файловые ресурсы, находящиеся на жестком магнитном диске;
- файловые ресурсы, находящиеся на флэш-накопителях.

В ИСПДн КБ разрешено постоянное хранение ПДн на жестком магнитном диске.

В штатном режиме работы ИСПДн КБ хранимая информация обрабатывается с использованием локальных ресурсов ПЭВМ.

1.3.5. Характеристика обрабатываемой входной и выходной информации

Характеристика обрабатываемой информации приведена в таблице 1.

Таблица 1 - информация, обрабатываемая в ИСПДн КБ.

Информация	Характеристика	Уровень конфиденциальности
Сведения о сотрудниках государственного предприятия	ФИО	ПДн
	Дата рождения	ПДн
	Серия, номер паспорта	ПДн
	Место работы	ПДн
	Табельный номер	ПДн

Характеристика входной информации ИСПДн КБ приведена в таблице 2.

Таблица 2 - входная информация ИСПДн КБ.

Информация	Характеристика	Уровень конфиденциальности	Источник информации
Зарплатный реестр	ФИО	ПДн	Субъект ПДн
	Дата рождения	ПДн	Субъект ПДн
	Серия, номер паспорта	ПДн	Субъект ПДн
	Место работы	ПДн	Субъект ПДн
	Табельный номер	ПДн	Субъект ПДн
	Номер счета в банке	ПДн	Субъект ПДн
	Сумма для перечисления	ПДн	Субъект ПДн

Характеристика выходной информации ИСПДн КБ приведена в таблице 3.

Таблица 3 - выходная информация ИСПДн КБ.

Информация	Характеристика	Уровень конфиденциальности	Источник информации
Выписка из банка	Номер счета	-	Банк
Выписка из банка	Остаток на счете	-	Банк
Зарплатный реестр	зашифрованный пакет информации, переданный в банк по общедоступным каналам связи	-	Субъект ПДн

1.4. Определение уровня защищенности ИСПДн КБ

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.

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.

В «ИСПДн КБ» обрабатывается и хранится информация, не составляющая государственную тайну, поэтому категорирование объекта информатизации не производится.

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

На основе акта классификации ИСПДн КБ (Приложение В) было выявлено что «ИС ПДн КБ» имеет 4-й уровень защищенности персональных данных.

1.5. Вывод по первой главе

В ходе проведения обследования объекта информатизации была дана характеристика «Информационной системе персональных данных клиент-банка» в УИТ государственного предприятия, характеристика комплекса используемых технических средств, характеристика используемого программного обеспечения. Также были описаны режимы работы, даны краткое описание технологического процесса и характеристика обрабатываемой входной и выходной информации.

Установили уровень защищенности ИСПДн КБ.

На основе анализа технического задания было принято решение об аттестации ИСПДн КБ.

2. АНАЛИЗ ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ

2.1. Анализ технологического процесса

2.1.1. Общие сведения

Технологический процесс обработки информации в «ИСПДн КБ» состоит из следующих стадий:

– управление доступом пользователей к ресурсам ИСПДн КБ;

– подготовка к обработке информации в ИСПДн КБ;

– обработка информации в ИСПДн КБ - осуществляется с помощью прикладного программного обеспечения;

– формирование выписок по счетам;

– отправка зарплатных реестров в ИСПДн КБ;

– обновление ПО и антивирусных баз;

– устранение сбоев аппаратного и программного обеспечения;

– проверка работы СЗИ НСД, включая просмотр событий и журналов аудита ОС, журналов СЗИ и антивирусного ПО администратором ИБ.

Описание технологического процесса обработки информации в ИСПДн КБ представлено в приложении Б.

2.1.2. Состав субъектов доступа и их функции

В ИСПДн КБ можно выделить следующие группы субъектов доступа:

– пользователи ИСПДн;

– администраторы (функции администратора ИБ и системного администратора объединены);

– технический персонал.

Пользователи допускаются к работе в ИСПДн на основании распоряжения о назначении пользователей, который утверждается начальником УИТ государственного предприятия.

Пользователи ИСПДн КБ имеют доступ только к программным ресурсам рабочей станции и информационным ресурсам ИСПДн КБ. При этом они не имеют возможности изменять настройки ОС, СЗИ НСД и антивирусного ПО.

Пользователи ИСПДн КБ выполняют следующие функции в системе:

– ввод данных в ПО (внесение зарплатных реестров) и передача их в банк по шифрованным каналам связи;

– вывод информации на печать;

– резервное копирование реестров.

Администраторы имеют полные права к программным и аппаратным ресурсам ИСПДн КБ, включая их настройки.

Администраторы не участвуют в технологическом процессе обработки конфиденциальной информации.

Администраторы выполняют следующие функции в ИСПДн КБ:

– настройка и конфигурирование ОС, СЗИ НСД и антивирусного ПО;

– обновление антивирусных сигнатур;

– анализ журналов безопасности;

– предоставление доступа субъектам доступа к ресурсам ИСПДн КБ;

– резервирование и восстановление информации;

– восстановление ИСПДн КБ в случае сбоя программного обеспечения;

– восстановление ИСПДн КБ в случае сбоя аппаратного обеспечения (совместно с техническим персоналом).

Выполненные работы администраторы обязаны фиксировать в журнале учета работы и технического обслуживания ПЭВМ.

Администраторы допускаются к работе в ИСПДн КБ на основании приказа по предприятию, утвержденного заместителем генерального директора по безопасности.

Технический персонал не участвует в технологическом процессе обработки конфиденциальной информации. Технический персонал допущен только к

аппаратным ресурсам ИСПДн КБ. Выполненные работы технический персонал обязан фиксировать в журнале учета работы и технического обслуживания ПЭВМ.

Технический персонал выполняет следующие функции:

- замену картриджа принтера;
- ремонт и обслуживание аппаратных ресурсов ИСПДн КБ.

Технический персонал допускается к работе в ИСПДн КБ на основании приказа по предприятию, утвержденного заместителем генерального директора по безопасности.

2.2. Анализ угроз и оценка риска

2.2.1. Правовая основа анализа угроз и оценки риска

Анализ угроз и оценка риска, были проведены на основании следующих документов:

– «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденная 14 февраля 2008 заместителем директора ФСТЭК России;

– «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденная 15 февраля 2008 заместителем директора ФСТЭК России;

– «Методические рекомендации по составлению частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждений здравоохранения, социальной сферы, труда и занятости», согласованная с начальником 2 управления ФСТЭК России 22.12.2009 г.

– «Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости», согласованная с начальником 2-го управления ФСТЭК России 22.12.2009 г.

2.2.2. Потенциальные угрозы безопасности персональных данных

Угрозы безопасности ПДн рассматриваются в соответствии с «Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной заместителем директора Федеральной службой по техническому и экспортному контролю России 15 февраля 2008 года.

По видам возможных источников угроз в ИСПДн КБ рассмотрены угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющих доступ к ИСПДн КБ, включая пользователей ИСПДн КБ, реализующих угрозы непосредственно в ИСПДн КБ.

По структуре ИСПДн КБ, на которые направлена реализация угрозы безопасности ПДн, рассмотрены угрозы безопасности ПДн, обрабатываемых в ИСПДн КБ на базе локальных информационных систем.

По виду несанкционированных действий, осуществляемых с ПДн, рассмотрены угрозы:

– приводящие к нарушению конфиденциальности ПДн (копированию или несанкционированному распространению), при реализации которых не осуществляется непосредственного воздействия на содержание информации;

– приводящие к несанкционированному, в том числе случайному, воздействию на содержание информации, в результате которого осуществляется изменение ПДн или их уничтожение;

– приводящие к несанкционированному, в том числе случайному, воздействию на программные или программно-аппаратные элементы ИСПДн КБ, в результате которого осуществляется блокирование ПДн.

По виду каналов, с использованием которых реализуются угрозы безопасности ПДн, рассмотрены:

– угрозы, реализуемые через каналы, возникающие за счет использования технических средств съема (добывания) информации, обрабатываемой в технических средствах ИСПДн или ВТСС (технические каналы утечки);

– угрозы, реализуемые за счет несанкционированного доступа к ПДн в ИСПДн с использованием штатного ПО ИСПДн или специально разрабатываемого ПО.

2.2.3. Источники угроз ИСПДн КБ

Источниками угроз для ИСПДн КБ являются:

– нарушитель;

– вредоносная программа;

– аппаратная закладка.

По наличию права постоянного или разового доступа в 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.

Так как ИСПДн КБ функционирует на базе ПЭВМ подключенной к сетям связи общего пользования и сетям международного информационного обмена через сертифицированный межсетевой экран Cisco ASA 5540 (сертификат № 3677 от 30.11.2016, действителен до 30.11.2019), возможности внешнего нарушителя не рассматриваются.

Внутренние потенциальные нарушители подразделяются на восемь категорий в зависимости от способа доступа и полномочий доступа к ПДн.

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

Ниже перечислены категории возможных внутренних нарушителей:

– лица, имеющие санкционированный доступ к ИСПДн КБ, но не имеющие доступа к ПДн;

– зарегистрированные пользователи ИСПДн КБ, осуществляющие ограниченный доступ к ресурсам ИСПДн КБ с рабочего места;

– зарегистрированные пользователи с полномочиями администратора ИСПДн КБ;

– зарегистрированные пользователи с полномочиями администратора безопасности ИСПДн КБ;

– программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте;

– разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на ИСПДн КБ.

2.2.4. Потенциальные угрозы безопасности информации

Основную угрозу безопасности ИСПДн представляют преднамеренные действия вероятных нарушителей.

В соответствии с требованиями «Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», рассчитан уровень исходной защищенности ИСПДн КБ на основе показателей исходной защищенности, приведенных в таблице 4.

Таблица 4 – Показатели исходной защищенности ИСПДн КБ.

№	Технические и эксплуатационные характеристики ИСПДн КБ	Уровень защищенности
1	2	3
1.	По территориальному размещению: ИСПДн, развернутая в пределах контролируемой зоны	Высокий
2.	По наличию соединения с сетями общего пользования: ИСПДн КБ, отделена от сети общего пользования с помощью сертифицированного межсетевого экрана	Высокий
3.	По встроенным (легальным) операциям с записями баз персональных данных: запись, удаление, сортировка	Средний
4.	По разграничению доступа: ИСПДн, в которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн КБ	Средний

Продолжение таблицы 4

1	2	3
5.	По наличию соединений с другими базами данных иных ИСПДн: ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	Высокий
6.	По уровню обобщения (обезличивания) ПДн: ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	Низкий
7.	По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки: ИСПДн, не предоставляющие никакой информации	Высокий

Из таблицы 4 видно, что четыре показателя (57%) имеют значение «Высокий», два показателя (29%) имеют значение «Средний» и один показатель (14%) имеет значение «Низкий».

«ИСПДн КБ» имеет средний уровень исходной защищенности (Y1 = 5), т.к. не менее 70% характеристик соответствуют уровню не ниже «Средний».

При составлении перечня актуальных угроз безопасности ПДн каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент Y2:

– 0 для маловероятной угрозы;

– 2 для низкой вероятности угрозы;

– 5 для средней вероятности угрозы;

– 10 для высокой вероятности угрозы.

Коэффициент реализуемости угрозы Y определяется соотношением: $Y = (Y1 + Y2)/20$. По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

– если $0 \leq Y \leq 0,3$, то возможность реализации угрозы признается низкой;

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

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

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

При оценке опасности угрозы на основе опроса экспертов определяется вербальный показатель, который имеет три значения:

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

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

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

Актуальность каждой угрозы определяется в соответствии с правилами, указанными в таблице 5.

Таблица 5 – Правила отнесения угрозы безопасности ПДн к актуальной.

Возможность реализации угрозы (Y)	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Перечень потенциальных угроз безопасности информации в «ИСПДн», их опасность и актуальность приведены в частной модели угроз в приложении Д.

Актуальными являются угрозы:

– просмотр информации на дисплее сотрудниками, не допущенными к обработке персональных данных;

– просмотр информации на дисплее посторонними лицами, находящимися в помещении в котором ведется обработка персональных данных;

– просмотр информации на дисплее посторонними лицами, находящимися за пределами помещения в котором ведется обработка персональных данных

– хищение съемных накопителей;

– модификация, уничтожение информации;

– несанкционированный доступ к информации при техническом обслуживании узлов ПЭВМ;

– непреднамеренное отключение средств защиты;

– выход из строя аппаратных средств;

– сбой системы электроснабжения;

– доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке;

– разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке.

2.3. Меры по обеспечению безопасности ПДн

Для нейтрализации представленных угроз приняты организационные и программно-технические меры, представленные в частной модели угроз (Приложение Д).

2.3.1. Организационные меры

Организационными мерами по обеспечению безопасности информации ИСПДн КБ являются:

– обеспечение защиты информационных ресурсов от хищения, утраты, утечки, уничтожения, искажения или подделки за счет несанкционированного доступа и специальных воздействий;

– обеспечение санкционированного доступа в ИС уполномоченным пользователям.

В рамках указанных направлений политики обеспечения безопасности информации осуществляются:

– реализация разрешительной системы доступа исполнителей (пользователей, обслуживающего персонала) к работам, документам и информации конфиденциального характера;

– реализация системы инженерно-технических и организационных мер охраны, предусматривающей комплексное применение современных технических средств охраны, обнаружения, наблюдения, сбора и обработки информации, обеспечивающих достоверное отображение и объективное документирование событий;

– ограничение доступа посторонних лиц:

1. в помещения, где размещены средства информатизации, на которых обрабатывается (хранится, передается) конфиденциальная информация;

2. непосредственно к самим средствам информатизации и коммуникациям;

– разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации в подсистемах различного уровня и назначения, входящих в ИС с учетом принципа минимальной достаточности – наделение каждого пользователя минимально необходимыми для выполнения ими своих функциональных обязанностей полномочиями по доступу к ресурсам ИС;

– учет документов, информационных массивов, регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;

– предотвращение внедрения в ИС программ-вирусов, программных закладок;

– надежное хранение традиционных и машинных носителей информации, паролей (ключей, ключевой документации) и их обращение, исключающее хищение, подмену и уничтожение;

– необходимое резервирование технических средств и дублирование массивов и носителей информации.

2.3.2. Программно-технические меры

Для защиты ПДн используются, в качестве СЗИ НСД, штатные средства сертифицированной операционной системы Windows 7 а также приняты следующие меры:

– для получения доступа к рабочему столу необходимо ввести имя пользователя и пароль;

– пользователям рабочей станции, работающей в среде ОС Windows,

установлены экранные заставки с паролем;

– для защиты рабочей станции от вирусов используется антивирусное ПО.

Применение сертифицированных по требованиям безопасности информации технических – средств активного зашумления для ИСПДн КБ не требуется, поскольку данный объект информатизации размещен в пределах контролируемой зоны – приказ, утвержденный генеральным директором № 146/279-А от 09.03.2018.

2.4. Реализация политик безопасности.

Защита информации в ИСПДн КБ обеспечивается на всех этапах обработки информации и во всех режимах функционирования, в том числе, и на стадии внедрения и при проведении ремонтно-профилактических работ.

В качестве ПО ИСПДн КБ используются только штатные программные средства. Средства разработки и отладки программ исключены из программной конфигурации программного обеспечения.

СЗИ НСД в ИСПДн КБ основывается на положениях и требованиях существующих законов, стандартов и нормативно-методических документов по защите от НСД к информации, действующих в государственном предприятии.

При защите ПДн в используют сертифицированные СЗИ НСД.

С целью предотвращения внедрения в ИСПДн КБ программ-вирусов, программных закладок и прочего вредоносного ПО на рабочей станции используется лицензионное антивирусное и системное ПО.

Запрещается передавать ПДн посторонним лицам вербально, в бумажном и электронном виде.

Проводится учёт всех носителей информации с помощью их маркировки и с занесением учётных данных в журнал. Учёт защищаемых носителей должен проводиться в журнале с регистрацией их выдачи.

Во время неиспользования отчуждаемые носители информации хранятся в сейфе. Запрещается копировать информацию на неучтённые носители

информации. Нарушители требований по защите информации привлекаются к дисциплинарной ответственности.

Для минимизации времени восстановления наиболее критичных элементов системы выполняется их резервное копирование. Процесс восстановления из резервных копий документирован.

Размещение мониторов максимально затрудняет возможность ознакомления с отображаемой на них информацией посторонними лицами. Используются экранные заставки. Пользователь должен блокировать компьютеры при выходе из помещения. Дверь помещения оборудована механическим замком.

Права пользователям ИС предоставляются исходя из принципа минимальной достаточности. Пароль имеет длину не менее шести символов и меняется не реже раза в год.

Для исключения несанкционированной установки оборудования, корпусы компьютеров опечатываются специальными наклейками. Проводится периодический мониторинг аппаратной и программной конфигурации компьютера. Обязательно использование антивирусного программного обеспечения. Все изменения в ИС документируются.

Определен круг ответственности и назначены ответственные за обеспечение безопасности ПДн.

Оправка зарплатных реестров осуществляется только после подписания их электронно-цифровой подписью.

Оправка зарплатных реестров осуществляется только с помощью специального программного обеспечения «Клиент-банк».

Подключение к общедоступным сетям осуществляется через сертифицированный межсетевой экран 5510 Cisco ASA 5540 (сертификат № 3677 от 30.11.2016, действителен до 30.11.2019).

Доступ из общедоступных сетей к ПЭВМ запрещен правилами на межсетевом экране.

2.5. Разработка программы и методики аттестационных испытаний.

По результатам анализа исходных данных аттестуемого объекта информатизации разработана программа аттестационных испытаний (Приложение К). Она была разработана на основе порядка защиты конфиденциальной информации, описанного в документе «Специальные требования и рекомендации по технической защите конфиденциальной информации».

Документ «Программа и методики аттестационных испытаний информационной системы персональных данных клиент-банка» предусматривает перечень работ и их продолжительность, методики испытаний, определяются количественный и профессиональный состав аттестационной комиссии, назначаемой органом по аттестации объекта информатизации, необходимость использования контрольной аппаратуры и тестовых средств на аттестуемом объекте информатизации.

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».

Задачей аттестационных испытаний является оценка защищенности ИСПДн 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.

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.

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.

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.

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.

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

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.

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 орган по аттестации;

– проведение дополнительных испытаний по дополнительному соглашению;

– применение дополнительных организационно-технических мер защиты.

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

2.6. Вывод по второй главе

В ходе данного этапа были проанализированы следующие документы:

– описание технологического процесса обработки информации объекта информатизации УИТ государственного предприятия;

– частная модель угроз и требования к системе защиты;

– технологическая инструкция администратора ИБ;

– технологическая инструкция по обеспечению защиты при работе в информационных системах, обрабатывающих конфиденциальную информацию;

– технологическая инструкция для технического обслуживающего персонала;

Выявлены состав субъектов и их функции, произведены анализ угроз и оценка риска объекта информатизации, рассмотрены основные положения политики безопасности ИСПДн КБ и рекомендации по реализации политик безопасности. Разработан документ «Программа и методики проведения аттестационных испытаний» (Приложение И).

3.ЭТАП АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ

3.1. Меры по обеспечению безопасности персональных данных и способы их реализации

В соответствии с «Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных приказом ФСТЭК России от 18 февраля 2013 г. № 21 был проведен анализ мер по обеспечению безопасности персональных данных и способы их реализации.

Меры по обеспечению безопасности ПДн, соответствующие 4-му уровню защищенности ПДн, а также способы их реализации с помощью СЗИ НСД, применяемых в «ИСПДн КБ» приведены в таблице 6:

Таблица 6 – Реализация мер по обеспечению безопасности ПДн в ИС.

№	Содержание мер по обеспечению безопасности ПДн.	Способ реализации (компенсирующие меры)
1	2	3
Идентификация и аутентификация субъектов доступа и объектов доступа.		
1.	Идентификация и аутентификация пользователей, являющихся работниками оператора.	Средствами СЗИ НСД и ОС осуществляется идентификация и аутентификация пользователей и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей. Каждый пользователь (включая администраторов) ИС имеет свою учетную запись в ОС. Аутентификация пользователя осуществляется с использованием паролей.
2.	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов.	Приказом назначены администраторы ИБ. Инструкцией администратора ИБ определен порядок управления идентификаторами. Идентификаторы пользователям присваиваются на основании утвержденного списка.

Продолжение таблицы 6

1	2	3
3.	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации.	Приказом назначены администраторы ИБ. Инструкцией администратора ИБ определен порядок управления средствами аутентификации.
4.	Защита обратной связи при вводе аутентификационной информации.	В процессе аутентификации обеспечивается исключение отображения для пользователя действительного значения аутентификационной информации (пароля).
5.	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей).	В ИС отсутствуют пользователи, не являющиеся работниками оператора.
Управление доступом субъектов доступа к объектам доступа (УПД)		
1.	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	Приказом назначены администраторы ИБ. Инструкцией администратора ИБ определен порядок управления учетными записями пользователей. Учетные записи пользователям (работникам оператора) присваиваются на основании утвержденного списка. В ИС отсутствуют пользователи, не являющихся работниками оператора
2.	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	Управление доступом субъектов доступа к объектам доступа реализованы средствами СЗИ НСД на основании утвержденных списков пользователей.
3.	Управление информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	Подключение к сети Интернет производиться через сертифицированный межсетевой экран.

Продолжение таблицы 6

1	2	3

4.	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Приказами назначены администраторы и технический персонал. Полномочия пользователям (работникам оператора) присваиваются на основании утвержденного списка пользователей. Разделение полномочий пользователей и администраторов выполняется настройками и созданием локальных групп в ОС. Функции администраторов, пользователей и технического персонала определены технологическим процессом обработки информации и соответствующими инструкциями.
5.	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Права пользователям назначаются исходя из принципа минимальной достаточности с помощью средств и настроек ОС и СЗИ НСД. На рабочей станции пользователей установлено ПО исходя из принципа минимальной достаточности. Настройки СЗИ НСД зафиксированы в формуляре.
6.	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	Настройками СЗИ НСД установлено ограничение неуспешных попыток.
7.	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	Подключение производится через сертифицированный межсетевой экран. Доступ из общедоступных сетей к ПЭВМ запрещен правилами на межсетевом экране.
8.	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	Использование в ИС технологий беспроводного доступа не применяется и запрещено средствами СЗИ НСД.
9.	Регламентация и контроль использования в информационной системе мобильных технических средств	Использование в ИС мобильных технических средств не применяется и запрещено средствами СЗИ НСД.

10.	Управление взаимодействием с информационными системами сторонних организаций.	Осуществляется через ПО «Клиент-банк» с применением криптографических средств защиты.

Продолжение таблицы 6

1	2	3
	Регистрация событий безопасности	
1.	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	Средствами ОС и СЗИ НСД настроен аудит (вход/выход, регистрация запуска программ, подключение отчуждаемых МНИ и пр.). Журналы безопасности проверяются администраторами ИБ в сроки, установленные инструкциями.
2.	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	Средствами ОС и СЗИ НСД настроен аудит (вход/выход, регистрация запуска программ, подключение съемных МНИ и пр.). Журналы безопасности проверяются администраторами ИБ в сроки, установленные инструкциями.
3.	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	Средствами ОС и СЗИ НСД осуществляется сбор и сохранение информации о событиях безопасности (аудита). Журналы безопасности сохраняются администраторами ИБ после выполнения проверки.
4.	Защита информации о событиях безопасности	К журналам безопасности имеют доступ только администраторы ИБ, назначенные приказом.
	Антивирусная защита	
1..	Реализация антивирусной защиты	В ИС обеспечивается антивирусная защита, включающая обнаружение компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.
2.	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	С периодичностью, определенной инструкцией, администратор ИБ осуществляет обновление антивирусных БД.

Продолжение таблицы 6

1	2	3
Контроль защищенности персональных данных.		
1.	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.	Установка обновлений ПО, включая СЗИ НСД выполняется только администраторами ИБ на основании утвержденного технического решения.
Защита технических средств.		
1.	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	Обеспечивается контроль и управление физическим доступом к техническим средствам, средствам ЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к ним. Проводятся обследования помещений с выпуском актов. Утверждены списки лиц допущенных к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.
2.	Размещение устройств вывода информации, исключающее ее несанкционированный просмотр.	Размещение устройств вывода (отображения, печати) информации исключают возможность несанкционированного просмотра выводимой информации лицами, не допущенными к ней, как из-за пределов КЗ, так и в пределах КЗ.
Защита информационной системы, ее средств, систем связи и передачи данных.		
	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по	Беспроводные каналы связи не используются и запрещены настройками СЗИ НСД.

	каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	

Исходя из проделанного анализа, можно сделать вывод, что предлагаемые организационно-технические меры защиты информации обеспечивают требования 4-го уровня защищённости ПДн и полностью соответствуют требованиям, предъявляемым к данным ИСПДн КБ.

3.2. Аттестационные испытания

Аттестационные испытания ИСПДн проводились в соответствии «Программой и методикой проведения аттестационных испытаний».

Аттестационные испытания содержали 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.

В соответствии с разработанной «Программой и методикой проведения аттестационных испытаний» провели испытания следующих подсистем по защите информации от несанкционированного доступа к ИСПДн:

– подсистемы управления доступом;

– подсистемы регистрации и учёта, контроля целостности и антивирусной защиты на соответствие требованиям руководящих документов по защите информации.

В процессе испытаний использовалась программа фиксации и контроля исходного состояния программного комплекса «ФИКС»;

По результатам оценки были оформлены протоколы аттестационных испытаний объекта информатизации «ИСПДн КБ» УИТ государственного предприятия на соответствие требованиям по защите информации от несанкционированного доступа (Приложение Л) и организационным требованиям по защите информации (Приложение К). На основе этих протоколов было оформлено заключение по результатам аттестационных испытаний. Заключение по результатам аттестационных испытаний представлено в приложении М.

Аттестационная комиссия посчитала, что реализованные средства и меры защиты достаточны и соответствуют требованиям действующих нормативных документов по безопасности информации. Таким образом, на аттестуемую ИСПДн КБ был выдан аттестат соответствия на право обработки ПДн в соответствии с установленным уровнем защищенности и сроком на три года (Приложение Н).

4.БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

4.1. Введение

Аттестация системы защиты информации сложный и трудоемкий процесс, связанный с работой на персональных электронно-вычислительных машинах, а также с прочими электрическими приборами. Для того чтобы избежать негативных последствий в процессе работы над проектом по аттестации системы защиты информации необходимо руководствоваться определенными правилами и соблюдать необходимые требования, которые мы и рассмотрели в настоящей главе.

4.2. Рекомендации по организации рабочего места пользователя

Организация рабочего места с электронно-вычислительной техникой начинается с выбора помещения и его соответствия требованиям нормативным документам. Так, в СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы» приведены основные требования к таким помещениям.

К основным пунктам относятся:

– в помещения должно присутствовать естественное и искусственное освещение, которые должны соответствовать требования нормативной документации;

– площадь на одно рабочее место пользователей ПЭВМ с ВДТ на базе плоских дискретных экранов (жидкокристаллические, плазменные) должно быть– 4,5 $м^2$;

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

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

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

4.2.1. Требования к помещениям для размещения рабочего места

В производственных помещениях, в которых работа с использованием ПЭВМ является основной и связана с нервно-эмоциональным напряжением, должны обеспечиваться оптимальные параметры микроклимата для категории работ 1а в соответствии с действующими санитарно-эпидемиологическими нормативами микроклимата производственных помещений.

Для определения микроклимата производственного помещения воспользуемся нормативным документом СанПиН 2.2.4.3359-16 «Санитарно-эпидемиологические требования к физическим факторам на рабочих местах». Оптимальные условия микроклимата для работ класса 1а приведены в Таблице 19.

Таблица 7 – Гигиенические требования к микроклимату в помещениях.

Период года.	Категория работ по уровням энерго-затрат, Вт.	Температура воздуха, ^{0}С.	Температура поверхностей, ^{0}С.	Относительная влажность воздуха, %.	Скорость движения воздуха, м/с.
Холодный	1а (до 139)	22-24	21-25	60-40	0,1
Теплый	1а (до 139)	23-25	22-26	60-40	0,1

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

4.2.2. Требования к уровням шума на рабочих местах

В нормативном документе СанПиН 2.2.4.3359-16 «Санитарно-эпидемиологические требования к физическим факторам на рабочих местах» описывается допустимый уровень шума на рабочих местах, при работе на электронно-вычислительных машинах на производстве.

По характеру спектра шум бывает:

– Тональный;

– Широкополосный.

Нормативным эквивалентным уровнем звука на рабочих местах (за исключением рабочих мест является 80 дБА). В случае превышения уровня шума на рабочем месте выше 80 дБА, работодатель должен провести оценку риска здоровью работающих и подтвердить приемлемый риск здоровью работающих.

Измерения уровней шума проводятся в соответствии с законодательством Российской Федерации.

При работе на электронно-вычислительной машине источником шума являются:

– источник бесперебойного питания;

– системный блок ПЭВМ;

– работающие принтеры и многофункциональные устройства.

4.2.3. Требования к освещению на рабочих местах

Правильно настроенное освещение рабочего места, является неотъемлемым фактором при организации работы за электронно-вычислительными машинами. Правильно настроенным и сбалансированным освещением рабочего места является совокупность естественного и искусственного освещения. Чтобы правильно наладить освещение рабочего места необходимо руководствоваться нормативным документом СанПиН 2.2.2/2.4.1340-

03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы».

В нормативном документе указаны следующие требования к освещенности:

– рабочие столы следует размещать таким образом, чтобы ВДТ были ориентированы боковой стороной к световым проемам, чтобы естественный свет падал преимущественно слева;

– искусственное освещение в помещениях для эксплуатации ПЭВМ должно осуществляться системой общего равномерного освещения;

– в производственных и административно-общественных помещениях, в случаях преимущественной работы с документами и бумагами, следует применять системы комбинированного освещения.

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

Для освещения помещений с ПЭВМ рекомендуется применять светильники с зеркальными параболическими решетками, укомплектованными электронными пуско-регулирующими аппаратами (ЭПРА). Общее освещение при использовании люминесцентных светильников следует выполнять в виде сплошных или прерывистых линий светильников, расположенных сбоку от рабочих мест, параллельно линии зрения пользователя и линии оконных проёмов при рядном расположении рабочих мест, оснащённых ПЭВМ с ЖК - мониторами.

Для того, чтобы уровень освещенности находился всегда в пределах нормированных значений, необходимо проводить очистку стекол окон, своевременную замену ламп, а также содержание светильников в чистоте.

4.2.4. Требования к электробезопасности

По степени опасности поражения электрическим током согласно Правилам Устройства Электроустановок (ПУЭ) рабочее помещение относится к классу помещений с повышенной опасностью. Это обусловлено тем, что имеется

возможность прикосновения сотрудника к металлоконструкциям с заземлением сооружений и зданий и одновременно к металлическим элементам оборудования.

Учитывая тот факт, что доступ к токопроводящим элементам приборов затруднен, то причиной поражения электрическим током от прикосновения к устройству может стать нарушения изоляции токопроводящих элементов.

Для избегания подобного рода инцидентов необходимо производить постоянный контроль целостности оборудования, в частности состояния токопроводящих элементов. Перед началом работы следует осмотреть целостность изоляции шнуров, проводов, удлинителей (если таковые имеются).

Для предотвращения образования и защиты от статического электричества в помещениях с ПЭВМ необходимо использовать аэроионизаторы и увлажнители воздуха. В отделке помещений следует отдавать предпочтение антистатическим материалам. Полы должны иметь антистатическое покрытие.

Документом «Правила устройства электроустановок» предусмотрены следующие технические способы и средства защиты от поражения электрическим током:

– обеспечение недоступности токоведущих частей, находящихся под напряжением для случайного прикосновения;

– устранение опасности поражения при появлении напряжения на нетоковедущих частях электрооборудования посредствам зануления.

4.2.5. Организация режима труда и отдыха пользователя

Для организации режима труда при работе за электронно-вычислительной машиной необходимо руководствоваться СанПиН 2.2.2/2.4.1340-03[11]. По виду трудовой деятельности сотрудника отдела работу можно отнести к «В» классу. То есть, работа предусматривает как и ввод информации, так и ее считывание.

Для видов трудовой деятельности устанавливается три категории тяжести и напряженности работы с электронно-вычислительными машинами. Для группы

«В» по суммарному времени непосредственной работы с ВДТ и ПЭВМ за рабочую смену, но не более 6 часов за смену.

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

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

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

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

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

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

В случаях возникновения у пользователя зрительного дискомфорта и других неблагоприятных субъективных ощущений, несмотря на соблюдение санитарно-гигиенических, эргономических требований, режимов труда и отдыха следует применять индивидуальный подход в ограничении времени работ

с ЭВМ. Коррекцию длительности перерывов для отдыха или проводить смену деятельности на другую, не связанную с использованием ЭВМ.

4.3. Пожарная безопасность.

Все правила и требования в области обеспечения пожарной безопасности представлены в нормативном документе Постановление правительства №390 от 25.04.2012 «О Противопожарном режиме». Настоящие Правила противопожарного режима содержат требования пожарной безопасности, устанавливающие правила поведения людей, порядок организации производства и содержания территорий, зданий, сооружений, помещений организаций и других объектов (далее - объекты) в целях обеспечения пожарной безопасности.

Согласно данным правилам и требованиям, в отношении каждого объекта руководителем организации, в пользовании которой на праве собственности или на ином законном основании находятся объекты, утверждается инструкция о мерах пожарной безопасности в соответствии с требованиями настоящего документа.

Лица допускаются к работе на объекте только после прохождения обучения мерам пожарной безопасности.

Обучение лиц мерам пожарной безопасности осуществляется путем проведения противопожарного инструктажа и прохождения пожарно-технического минимума.

Порядок и сроки проведения противопожарного инструктажа и прохождения пожарно-технического минимума определяются руководителем организации. Обучение мерам пожарной безопасности осуществляется в соответствии с нормативными документами по пожарной безопасности.

Руководитель организации назначает лицо, ответственное за пожарную безопасность, которое обеспечивает соблюдение требований пожарной безопасности на объекте.

Во всех помещениях и зданиях предприятия должны располагаться специальные таблички с номеров вызова пожарной охраны, а также утвержденные планы эвакуации персонала.

На объекте с массовым пребыванием людей руководитель организации обеспечивает наличие инструкции о действиях персонала по эвакуации людей при пожаре, а также проведение не реже 1 раза в полугодие практических тренировок лиц, осуществляющих свою деятельность на объекте.

Запрещается курение на территории предприятия, не оборудованных табличками «Место для курения». Руководитель организации обеспечивает размещение на указанных территориях знаков пожарной безопасности "Курение табака и пользование открытым огнем запрещено".

Руководитель организации обеспечивает наличие на дверях помещений производственного и складского назначения и наружных установках обозначение их категорий по взрывопожарной и пожарной опасности, а также класса зоны в соответствии с главами 5, 7 и 8 Федерального закона "Технический регламент о требованиях пожарной безопасности".

Руководитель организации организует проведение работ по заделке негорючими материалами, обеспечивающими требуемый предел огнестойкости и дымо-газонепроницаемость, образовавшихся отверстий и зазоров в местах пересечения противопожарных преград различными инженерными (в том числе электрическими проводами, кабелями) и технологическими коммуникациями.

Следует отметить, что данный нормативный документ накладывает ряд запретов на организацию в области пожарной безопасности. К ним относятся:

– снимать предусмотренные проектной документацией двери эвакуационных выходов из поэтажных коридоров, холлов, фойе, тамбуров и лестничных клеток, другие двери, препятствующие распространению опасных факторов пожара на путях эвакуации;

– производить изменение объемно-планировочных решений и размещение инженерных коммуникаций и оборудования, в результате которых ограничивается доступ к огнетушителям, пожарным кранам и другим системам обеспечения

пожарной безопасности или уменьшается зона действия автоматических систем противопожарной защиты (автоматической пожарной сигнализации, стационарной автоматической установки пожаротушения, системы дымоудаления, системы оповещения и управления эвакуацией);

– загромождать мебелью, оборудованием и другими предметами двери;

– загромождать и закрывать проходы к местам крепления спасательных устройств.

Руководитель организации обеспечивает содержание наружных пожарных лестниц и ограждений на крышах зданий и сооружений в исправном состоянии, организует не реже 1 раза в 5 лет проведение эксплуатационных испытаний пожарных лестниц и ограждений на крышах с составлением соответствующего протокола испытаний, а также периодического освидетельствования состояния средств спасения с высоты в соответствии с технической документацией или паспортом на такое изделие.

Руководитель организации при выполнении планового ремонта или профилактического осмотра технологического оборудования обеспечивает соблюдение необходимых мер пожарной безопасности.

Руководитель организации в соответствии с технологическим регламентом обеспечивает выполнение работ по очистке вытяжных устройств (шкафов, окрасочных, сушильных камер и др.), аппаратов и трубопроводов от пожароопасных отложений.

Поскольку, в рабочем помещении присутствует электротехника, то, возможный пожар будет иметь Класс Е (пожар электроустановок). Пожары такого класса тушат инертными разбавителями и порошками.

В случае возникновения пожара, нам необходимо применить один из следующих видов пожаротушения.

Огнетушители порошковые – ОП - Используются при тушении пожаров класса А и В (дерево, бумага, краски и ГСМ). Запрещается применение для тушения электроустановок, находящихся под напряжением.

Огнетушители углекислотные - ОУ . Предназначены для тушения загораний веществ, горение которых не может происходить без доступа воздуха, загораний электроустановок, находящихся под напряжением не более 1000В, жидких и газообразных веществ (класс В, С).

К первичным средствам пожаротушения относятся спец. емкости с песком, лопаты, ведра, ломы, багры, асбестовые полотна, грубошерстные ткани и войлок, огнетушители.

Первичные средства пожаротушения размещаются в легкодоступных местах и не должны быть помехой при эвакуации персонала из помещений.

4.4. Основные характеристики помещения

Работа связана с управлением и обработкой данных. Площадь помещения 12 м^2, высота от пола до потолка 2,5 м. Площадь на одно рабочее место 12 м^2, а объём 30 м^3. В помещении расположено 1 рабочее место с монитором и персональным компьютером (ПК).

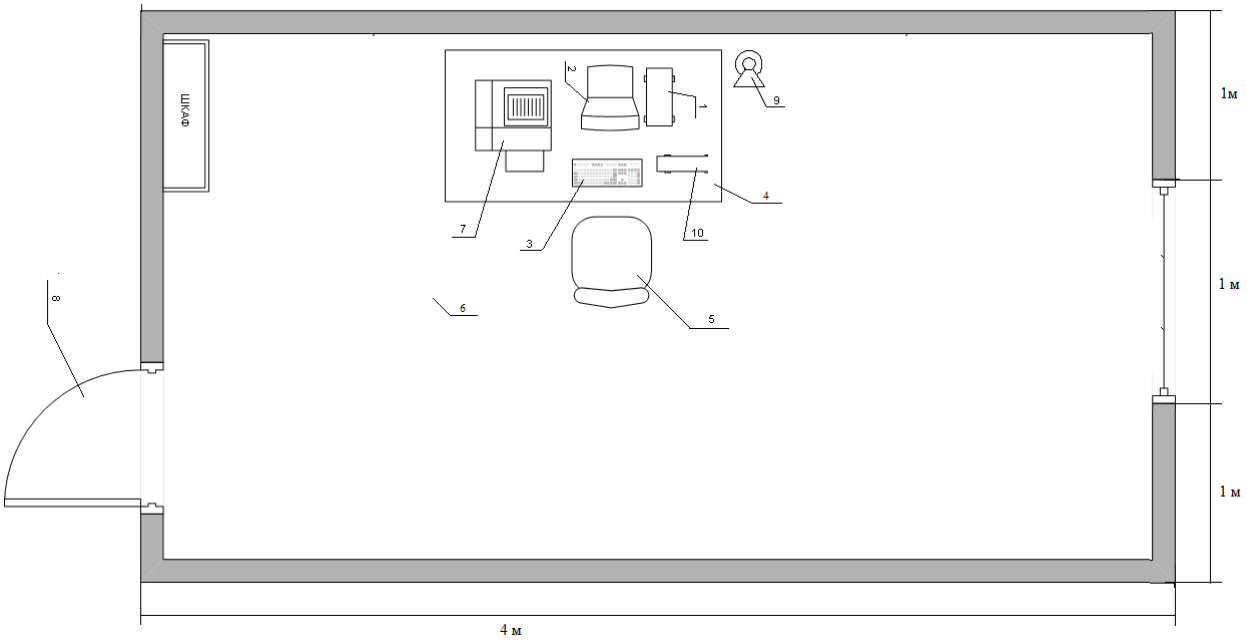

Рисунок 1 – Схема помещения УИТ.

1) системный блок ПК;
2) монитор;
3) клавиатура и мышь;

4) стол;

5) стул;

6) окно;

7) принтер;

8) дверь;

9) огнетушитель;

10) источник бесперебойного питания.

Помимо рабочего места, в помещении предусмотрен специальный шкаф для хранения накопителей на гибких магнитных дисках, бумаги и других расходных материалов.

Ниже приведена таблица соответствия характеристик рабочего места требуемым параметрам.

Таблица 8 - соответствие параметров рабочего места

№	Характеристика	Значение	Требуется
1.	Высота рабочего места	12 м2	4,5 м2
2.	Ширина рабочего места	550 мм	500 мм
3.	Глубина рабочего места на уровне колен	450 мм	450 мм
4.	Глубина рабочего места на уровне вытянутых ног	655 мм	650 мм
5.	Высота рабочего места	620 мм	600 мм
6.	Уровень шума	55 дБ	80 дБ
7.	Температура воздуха	24 С0	23-25 С0
8.	Температура поверхностей	23 С0	22-26 С0
9.	Относительная влажность воздуха	53 %	60-40 %
10.	Уровень энергозатрат	105 Вт	до 139 Вт

Параметры рабочего места соответствуют требуемым нормам. Компьютер, принтер, клавиатура и мышь установлены на компьютерном столе. Шумовых помех практически нет. Помещение с ЭВМ имеет естественное и искусственное освещение. Окно в помещении оборудовано регулируемыми горизонтальными жалюзи, что защищает устройства ЭВМ от прямого попадания солнечных лучей. Жалюзи изготовлены из металлической ленты серого цвета. Поверхность пола в помещении покрыта линолеумом бежевого цвета, который очень удобен для очистки и влажной уборки. Условия для работы, требующей повышенного внимания, удовлетворительные.

4.5. Вывод по четвертой главе

Вид человеческой деятельности, связанный с работой на производстве, работе на электронно-вычислительных машинах несет за собой множество опасных и вредных факторов, которые могут пагубно повлиять на здоровье человека, а значит и на его работоспособность и трудовую пригодность и эффективность.

Для того чтобы избежать влияния вредных факторов необходимо соблюдать нормы и требования стандартов в области безопасности жизнедеятельности. Следует уделять большое внимание и внутренним уставам и инструкциям, действующим на предприятии.

При работе над проектом по модернизации системы защиты информации мы будем использовать электронно-вычислительные машины, а также другие электроприборы. Ввиду этого, мы определили, что возможный пожар будет носить класса «Е». Для его тушения необходимо будет применить порошковые или инертные огнетушители. В качестве первичных средств пожаротушения следует использовать асбестовые полотна, ткани, обработанные специальным составом и песком.

Выполнение всех требований по безопасности позволит сделать трудовой процесс безопасным для здоровья, сберечь работоспособность, а значит повысить качество и быстроту выполнения трудовых заданий и обязанностей.

ЗАКЛЮЧЕНИЕ

В ходе выполнения выпускной квалификационной работы было произведено обследование объекта информатизации «Информационная система персональных данных клиент-банка» в управлении информационных технологий

государственного предприятия. ИСПДн КБ обрабатывает персональные данные абонентов, пользующихся дистанционными банковскими услугами.

В ходе обследования был проведен анализ организационно-распорядительных документов и установлен уровень защищенности ИСПДн КБ. Произведены анализ угроз и оценка риска объекта информатизации и приняты меры по реализации этих мер.

Разработан документ «Программа и методики проведения аттестационных испытаний». На основании этого документа были проведены аттестационные испытания на соответствия требованиям безопасности информации. Испытания проводились с использованием специальных средств проверки. ИСПДн КБ полностью соответствует этим требованиям. По результатам испытаний были оформлены протоколы аттестационных испытаний объекта информатизации «ИСПДн КБ» УИТ государственного предприятия на соответствие требованиям по защите информации от несанкционированного доступа и организационным требованиям по защите информации. На основе этих протоколов было оформлено заключение по результатам аттестационных испытаний.

В результате было принято решение о выдаче аттестата соответствия «Информационной системе персональных данных клиент-банка» в управлении информационных технологий государственного предприятия.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК.

Нормативно-правовые документы.

1. «Положение по аттестации объектов информатизации по требованиям безопасности информации» от 25.11.1994 // Консультант Плюс: Интернет-версия [Электронный ресурс] / ЗАО «Консультант Плюс». – М., 2018.

2. «Об утверждении доктрины информационной безопасности Российской Федерации»: указ Президента Российской Федерации от 05.12.2016 № 646 // Консультант Плюс Интернет-версия [Электронный ресурс] / ЗАО «Консультант». – М., 2018.

3. «О персональных данных»: федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ: (в ред. 22.02.2017) // Консультант Плюс : Интернет-версия [Электронный ресурс] / ЗАО «Консультант Плюс». – М., 2018.

4. «Об утверждении 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) // Консультант Плюс: Интернет-версия [Электронный ресурс] / ЗАО «Консультант Плюс». – М., 2018.

5. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»: постановление Правительства Российской Федерации от 01.11.2012 № 1119 // Консультант Плюс: Интернет-версия [Электронный ресурс] / ЗАО «Консультант Плюс». – М., 2018.

6. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15.02.2008 // Консультант Плюс: Интернет-версия [Электронный ресурс] / ЗАО «Консультант-Плюс». – М., 2018.

7. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 14.02.2008 // Консультант Плюс: Интернет-версия [Электронный ресурс] / ЗАО «Консультант Плюс». – М., 2018.

8. «Защита от несанкционированного доступа к информации Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей» : руководящий документ (Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. № 114) // ФСТЭК: Интернет-версия [Электронный ресурс]

9. СанПиН 2.2.2/2.4.1340-03. 2.2.2. Гигиена труда, технологические процессы, сырье, материалы, оборудование, рабочий инструмент. Гигиена детей и подростков. Гигиенические требования к персональным электронно-вычислительным машинам и организации работы. Санитарно-эпидемиологические правила и нормативы // Консультант Плюс: Интернет-версия [Электронный ресурс] / ЗАО «Консультант Плюс» – М., 2018.

10. СанПиН 2.2.4.3359-16. Санитарно-эпидемиологические требования к физическим факторам на рабочих местах. // КонсультантПлюс : Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – М., 2018.

11. ГОСТ Р 12.1.019-2009. Национальный стандарт Российской Федерации.

12. Система стандартов безопасности труда. Электробезопасность. Общие требования и номенклатура видов защиты – М.: Стандартинформ, 2010.

Основная литература.

1. Безопасность жизнедеятельности. / Под редакцией Н.А. Белова - М.: Знание, 2000 – 364 с.

2. Борьба с шумом на производстве: Справочник / Е.Я. Юдин, Л.А. Борисов; Под общей редакцией Е.Я. Юдина – М.: Машиностроение, 1985. – 400 с.

3. Дубовцев, В.А. Безопасность жизнедеятельности. / Учебное пособие для дипломников. - Киров: изд. КирПИ, 1992. – 213 с.

ПРИЛОЖЕНИЕ А

ГОСУДАРСТВЕННОЕ ПРЕДПРИЯТИЕ

УТВЕРЖДАЮ

Заместитель генерального
директора по безопасности

_____ С.В. Перфилов

____ . _____ . 2018

Информационная система персональных данных клиент-банка
Техническое задание

ЕЕ.338758.В20 1В

Начальник службы безопасности

_____ В.А. Кашуба

____ . _____ . 2018

Начальник управления
информационных технологий

_____ В.Е. Кочетков

___ . _____ . 2018

2018

1. Общие сведения

Настоящее техническое задание содержит основные требования к разработке и внедрению системы защиты информации в «Информационной системе персональных данных клиент-банка».

Наименование задачи – «Информационная система персональных данных клиент-банка» (далее – ИСПДн КБ).

Основным назначением задачи является передача платежных документов и зарплатных реестров в банки.

Комплекс технических средств состоит из компьютера, подключенного к сети Интернет и принтера.

Заказчиком задачи является УИТ государственного предприятия.

Высшая степень конфиденциальности информации, разрешенной к обработке в «ИСПДн КБ» - «персональные данные» (заключение ЭК № 675/5476 от 19.05.2018).

Информационной системе присвоен класс защищенности «уровень 4 персональных данных» в соответствии с актом классификации.

Исполнителем задачи является служба безопасности государственного предприятия.

2. Характеристика объекта

Назначением ИСПДн КБ является передача платежных документов и зарплатных реестров в банки, через сеть Интернет.

Функционирование ИСПДн КБ происходит по следующим этапам:

– получение файла выгрузки с платежными данными;

– подписание файла «второй» подписью;

– подписание файла «первой» подписью;

– отправка файла в банк.

Расположение ИС: г. Озерск, ул. Герцена 7, помещение № 226.

Режим обработки информации – многопользовательский, пользователи имеют одинаковые права доступа (полномочия) ко всей информации ИС, обрабатываемой и (или) хранимой на учтенных носителях.

Данная ИС находится в пределах контролируемой зоны. Границами контролируемой зоны являются стены здания (приказ о границах контролируемой зоны от 09.03.2018 № 146/279-А).

Входная информация поступает в виде файла с флэш-накопителя.

Выходная информация образуется в виде файлов отчетов полученных в информационной системе.

Данные работы выполняются на ПЭВМ, входящей в «ИСПДн КБ».

В состав программного обеспечения входит ПЭВМ:

– операционная система Microsoft Windows 7;

– офисное программное обеспечение Microsoft Office;

– программное обеспечение «Клиент-банк».

В системе выделены следующие группы пользователей:

– администратор информационной безопасности (далее - АИБ);

– пользователи;

– ремонтный персонал.

АИБ контролирует обслуживание, изменение конфигурации и модификацию программных и аппаратных средств, а также целостность программной среды, анализирует системный журнал.

АИБ формирует пароли пользователей системы, управляет доступом пользователей к ресурсам ИС. АИБ имеет полный доступ ко всей обрабатываемой информации. Все операции по управлению доступом АИБ фиксирует в «Журнале учета работы и обслуживания ПЭВМ».

Исполнители участвуют в технологическом процессе обработки информации, имеют доступ к программным ресурсам ИС, но не имеют доступа к аппаратным ресурсам, настройкам операционной системы.

Ремонтный персонал имеет доступ к аппаратным ресурсам ИС в присутствии АИБ. Ремонтный персонал не участвует в технологическом процессе обработки информации и не имеет доступа к защищаемой 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 к организационным мерам обеспечения безопасности информации

Для получения доступа в информационную систему пользователь должен ввести личные идентификационные данные (имя пользователя и пароль).

Требования к квалификации персонала:

– техническое обслуживание ПЭВМ должен выполнять персонал УИТ, прошедший обучение, сдавший экзамен на рабочее место и имеющий 3 группу по электробезопасности;

– системное обслуживание и обслуживание программного обеспечения осуществляют администраторы информационной безопасности из состава персонала УИТ, прошедшие соответствующее обучение.

Требования к допуску персонала к информации:

– допуск и доступ к информации пользователей ИС, АИБ и обслуживающего персонала УИТ должен осуществляться в соответствии с приказом «О назначении лиц….»;

– персонал отдела технического обслуживания УИТ должен быть включен в «Список лиц на допуск к ИСПДн КБ;

– пользователи, являющиеся пользователями ИС, должны быть назначены списком (распоряжением о назначении) пользователей, который утверждается руководителем подразделения государственного предприятия;

– администраторы информационной безопасности должны быть назначены приказом начальника заместителя генерального директора по безопасности;

– обязанности, права и ответственность пользователей, администраторов и обслуживающего персонала определяются соответствующими инструкциями.

Администраторы информационной безопасности отвечают за обеспечение безопасности информационной системы, за реализацию и непрерывность соблюдения установленных административных мер защиты и осуществляют постоянную организационную поддержку функционирования применяемых программных средств защиты, отвечают за функционирование ИС в установленном штатном режиме.

При выполнении работ в ИСПДн КБ пользователи должны руководствоваться инструкцией «Описание технологического процесса обработки конфиденциальной информации в ИСПДн КБ.

5. Требования к техническим средствам защиты информации

Требования по защите информации от НСД для ИС в соответствии с классом защищенности «уровень 4 персональных данных».

Подсистема управления доступом:

– должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

Подсистема регистрации и учета:

– должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова.

Подсистема обеспечения целостности:

– должна быть обеспечена целостность программных средств ОС, обрабатывающих информацию, а также неизменность программной среды;

– целостность программных средств осуществляется путем проведения верификации состава ПО;

– целостность программной среды обеспечивается отсутствием в ИС средств разработки и отладки программ;

– должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление, и контроль работоспособности.

6. Требования к физической защите

Должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и

здания, где размещается ИС, с помощью технических средств охраны и специального персонала, использование пропускного режима.

Продолжение приложения А

Помещение должно быть обследовано с составлением акта.

С целью контроля над входом в помещение лиц, входная дверь должна быть постоянно закрыта на кодовый замок. Код должен сообщаться только сотрудникам, постоянно работающим в помещении.

Должен быть определен порядок смены кода: кем осуществляется смена кода, периодичность смены кода, порядок оповещения о смене кода работающего персонала.

7. Требования к комплексу технических средств

Эксплуатация электрооборудования, входящего в состав ИС, должна проводиться в соответствии с правилами технической эксплуатации электроустановок потребителей ПТЭЭП, межотраслевыми правилами по охране труда (правилами безопасности) при эксплуатации электроустановок, локальными инструкциями по технике безопасности предприятия.

Для нормального функционирования ИС необходимо, чтобы ПЭВМ, входящие в ИС удовлетворяли следующим условиям:

– процессор не ниже Pentium-IV 2.2ГГц;

– оперативная память не менее 2048Мб;

– жесткий диск объемом не менее 250Гб.

8.Требования к технологическому процессу обработки информации

Технологический процесс работы в информационной системе должен быть подробно описан в инструкции «Описание технологического процесса обработки конфиденциальной информации в ИСПДн КБ».

Пользователи информационной системы выполняют ввод, обработку данных и формирование отчетных форм в ИСПДн КБ.

Сообщения, предоставляемые в ИСПДн КБ:

– системные сообщения ОС Windows 7 Professional;

– сообщения офисного программного обеспечения Microsoft Office;

– сообщения антивирусного программного обеспечения Kaspersky;

– сообщения программ «Клиент-Банк».

Подробное описание сообщений пользователю ИСПДн КБ приведены в документации на вышеуказанные программные продукты.

ПРИЛОЖЕНИЕ Б

ГОСУДАРСТВЕННОЕ ПРЕДПРИЯТИЕ

УТВЕРЖДАЮ

Заместитель генерального
директора по безопасности

_____ С.В. Перфилов

____ . _____ . 2018

Информационная система персональных данных клиент-банка
Описание технологического процесса обработки информации
объекта информатизации управления информационными технологиями
государственного предприятия

ЕЕ.338754.В20 РА

Начальник службы безопасности

_____ В.А. Кашуба

____ . _____ . 2018

Начальник управления
информационных технологий

_____ В.Е. Кочетков

___ . _____ . 2018

2018

Продолжение приложения Б

1. Введение

1.1. Информационная система персональных данных клиент-банка (далее – ИСПДн КБ) предназначена для приема и передачи документов (платежек, зарплатных реестров и т.п.) в банки, где открыты расчетные счета государственного предприятия.

1.2. Информационная система предназначена для обработки информации ограниченного распространения с пометкой «для служебного пользования» в информационно-вычислительной сети Интернет.

1.3. Комплекс технических средств состоит из компьютера, подключенного при помощи коммутационного оборудования в локальную вычислительную сеть.

1.4. В ИСПДн КБ обрабатывается служебная информация ограниченного распространения с пометкой «персональные данные» в виде файлов, созданных в пакетах прикладных программ.

1.5. Настоящий документ определяет технологический процесс (далее - ТП) обработки информации в ИСПДн КБ.

1.6. Задачами технологического процесса в ИСПДн КБ являются:

– управление доступом пользователей к ресурсам ИСПДн КБ;

– подготовка к обработке информации с пометкой «персональные данные»;

– обработка информации с пометкой «персональные данные»;

– прием и передача электронных сообщений в зашифрованном виде через сеть Интернет;

– завершение работ по обработке информации с пометкой «персональные данные»;

– резервное копирование и восстановление информации с пометкой «персональные данные»;

– обновление программного обеспечения;

– устранение сбоев аппаратного и программного обеспечения;

– проверка работы средств защиты информации, включая просмотр событий и журналов аудита ОС и антивирусного ПО администратором информационной безопасности (далее - АИБ).

1.7. На рабочие станции устанавливается системное ПО: сертифицированная по требованиям безопасности информации ОС Windows 7, пакет Microsoft Office исходя из принципа минимальной достаточности, программный комплекс "Клиент-банк", антивирусное ПО Kaspersky.

1.8. В качестве СЗИ от несанкционированного доступа в ИСПДн КБ используются встроенные средства операционной системы.

1.9. ИСПДн КБ является многопользовательской. Пользователи имеют одинаковые права доступа ко всей информации.

1.10. Настоящим технологическим процессом должны руководствоваться пользователи, участвующие в обработке информации с пометкой «персональные данные», администраторы информационной безопасности и администраторы ИСПДн КБ.

1.11. Администратор информационной безопасности имеет полный доступ ко всем системным и информационным ресурсам рабочих станций и серверов. Администратор ИСПДн КБ имеет доступ к установке нового ПО и модифицированию существующего, а также к настройке операционной системы в части, не касающейся безопасности. Функции администратора информационной безопасности и системного администратора в ИСПДн КБ совмещены.

2. Управление доступом пользователей к ресурсам ИСПДн КБ

2.1 Под управлением доступом к ресурсам ИСПДн КБ понимается назначение, изменение и удаление учетных реквизитов пользователей (имен и паролей), а также установка, изменение и прекращение прав пользователей на доступ к любым ресурсам (аппаратным, программным, информационным).

2.2 К ресурсам ИСПДн КБ и к защищаемой информации имеют доступ: администраторы ИСПДн КБ и аутентифицированный пользователь, осуществляющий ввод и корректировку информации. Только администратор ИСПДн КБ имеет доступ к настройкам безопасности системы, при этом он не участвует в технологическом процессе обработки информации.

3. Подготовка к обработке информации с пометкой «персональные данные»

3.1 Перед началом работы в ИСПДн КБ пользователю необходимо: убедиться в целостности устройств индикации вмешательства (пломбы, наклейки и т.п.) на используемой ПЭВМ.

3.1.2 Убедиться, что расположение монитора исключает возможность просмотра отображаемой информации посторонними лицами.

3.2 Далее пользователю необходимо выполнить вход в ИСПДн КБ и подключится к необходимым ресурсам. Для чего необходимо:

3.2.1 После включения рабочей станции и загрузки ОС, пользователю необходимо пройти процедуры идентификации и аутентификации, для чего после полной загрузки и нажатия комбинации клавиш Ctrl+Alt+Del, необходимо ввести идентификатор и пароль.

3.2.2 В случае если процедуру аутентификации пройти не удается, необходимо об этом сообщить администратору информационной безопасности.

3.2.3 Набор пароля на клавиатуре должен выполняться так, чтобы исключить его просмотр другими лицами.

3.3 Для работы с программным комплексом "Клиент-банк" необходимо его запустить и следовать инструкциям руководства пользователя на соответствующее программное обеспечение.

4. Обработка информации с пометкой «персональные данные»

Обработка информации пользователем осуществляется с помощью:

– пакета офисных программ – создание, редактирование документов с пометкой "персональные данные";

– прикладного программного обеспечения (выполняется в соответствии с руководством пользователя для прикладной программы).

5.Сохранение результатов обработки информации с пометкой «персональные данные»

Для сохранения результатов обработки информации пользователю необходимо выполнить следующие действия:

– в случае необходимости распечатать созданный (отредактированный) документ на принтере, с последующей постановкой учетных реквизитов – метки конфиденциальности;

– сохранить результаты работы в офисной программе - созданный (отредактированный) документ сохранить в хранилище пользователя на специально выделенном файловом ресурсе;

– сохранить результаты работы в прикладной программе.

6.Завершение работ по обработке информации с пометкой «персональные данные»

Перед тем как отлучиться с рабочего места (для временного отсутствия или по окончанию рабочей смены) пользователь ИСПДн КБ должен корректно завершить работу с программным обеспечением (по окончанию рабочей смены) и заблокировать (нажать комбинацию клавиш Ctrl+Alt+Del и кнопку "Блокировка рабочей станции") или выключить рабочую станцию («Пуск» – «Завершение работы» – «Выключить компьютер»).

Продолжение приложения Б

7. Резервное копирование и восстановление информации с пометкой «персональные данные»

С периодичностью, определенной соответствующей инструкцией администратор ИСПДн КБ должен выполнять резервное копирование информации, обрабатываемой в ИСПДн КБ с помощью прикладного ПО, либо вручную. Для этого необходимо:

Взять (получить под роспись) из сейфа учтенный отчуждаемый носитель информации.

Создать резервную копию информации на учтенный отчуждаемый носитель информации.

Убрать (сдать под роспись) в сейф учтенный отчуждаемый носитель информации.

В случае необходимости администратор должен выполнить восстановление информации, обрабатываемой в ИСПДн КБ с помощью прикладного ПО, либо вручную. Для этого необходимо:

– взять (получить под роспись) из сейфа учтенный отчуждаемый носитель информации;

– восстановить информацию с учтенного отчуждаемого носителя информации;

– убрать (сдать под роспись) в сейф, учтенный отчуждаемый носитель информации.

8.Обновление программного обеспечения

Под обновлением понимается замена ПО устаревшей версии на новую версию, а также обновление антивирусных баз данных, установка сертифицированных обновлений ОС, исправления и дополнения прикладной программы.

В процессе обновления ПО допускается ввод информации с лазерных, магнитных и отчуждаемых (flash-накопитель) носителей информации. Обновление ПО с лазерных, магнитных и отчуждаемых (flash-накопитель) носителей

информации осуществляется администратором ИСПДн КБ. Операция обновления фиксируется в "Журнале учета работы и технического обслуживания ПЭВМ".

Установку сертифицированных обновлений ОС, обновление антивирусных баз данных осуществляет администратор ИСПДн КБ. Операция обновления фиксируется в "Журнале учета работы и технического обслуживания ПЭВМ".

9. Устранение сбоев аппаратного и программного обеспечения

Под устранением сбоев аппаратного обеспечения понимается восстановление работоспособности, как отдельных элементов ПЭВМ, так и всей ПЭВМ в целом.

Устранением аппаратных сбоев занимается обслуживающий технический персонал ИСПДн КБ.

Под устранением сбоев программного обеспечения понимается восстановление части ПО (системного или прикладного) или полная переустановка системы (операционной системы, прикладных и общесистемных программ) путем форматирования жесткого магнитного диска и новой установки ПО.

Для защиты от сбоев должны быть приняты следующие меры:

– только администратор ИСПДн КБ имеет доступ к настройкам системы, связанным с безопасностью;

– включена антивирусная защита системы;

– администратор ИСПДн КБ обязан ежемесячно обновлять антивирусные программы.

Окончание приложения Б

ПРИЛОЖЕНИЕ В

ГОСУДАРСТВЕННОЕ ПРЕДПРИЯТИЕ

УТВЕРЖДАЮ

Заместитель генерального
директора по безопасности

_____ С.В. Перфилов

____ . _____ . 2018

Информационная система персональных данных клиент-банка
Акт классификации

№ 4.2.1/1915

Начальник службы безопасности

_____ В.А. Кашуба

____ . _____ . 2018

2018

Продолжение приложения В

Комиссия в составе: В.А. Кашуба, А.В. Евстигнеев, А.В. Куреннов, М.О. Бушуев провела работу по определению и присвоению уровня защищенности ИСПДн КБ, расположенной по адресу: г. Озерск, ул. Герцена, д. 7, кабинет № 226.

Рассмотрев исходные данные об информационной системе персональных данных, определила:

1) категория персональных данных: «Иные», т.к. ПДн не относятся к специальным, биометрическим и общедоступным;

2) количество субъектов персональных данных: менее 100000 человек;

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

4) наличие взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена: ИСПДн имеет соединение с сетями общего пользования.

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 клиент-банка» УИТ государственного предприятия присвоить уровень защищенности: четвертый (4).

Председатель комиссии	В.А. Кашуба
Члены комиссии:	А.В. Евстигнеев
	М.О. Бушуев
	А.В. Куреннов

Окончание приложения В

ПРИЛОЖЕНИЕ Г

ГОСУДАРСТВЕННОЕ ПРЕДПРИЯТИЕ

УТВЕРЖДАЮ

Заместитель генерального
директора по безопасности

_____ С.В. Перфилов

____ . _____ . 2018

Информационная система персональных данных клиент-банка
Технический паспорт

ЕЕ.14082.К58 КЭ

2018

Продолжение приложения Г

1. Общие сведения об объекте.

Наименование объекта: ИСПДн КБ государственного предприятия.

Расположение объекта: г. Озерск, ул. Герцена, д. 7, кабинет № 226.

Классификация объекта.

Уровень защищенности: 4 (четвертый).

2. Состав оборудования объекта.

Состав ОТСС приведен в таблице 1.

Таблица 1 – состав ОТСС

№	Наименование устройства	Модель	Заводской номер
1.	Системный блок	IRU Brava Home 114W	10157
2.	Монитор	Samsung S27A750D	ETL460C260723157E
3.	Клавиатура	Genius KM-122	ZM6C02019509
4.	Мышь	A4Tech X7 XL-750BX	130-130009-200
5.	МФУ	Samsung SCX-4100	CNKDS08892

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

Таблица 2 – Перечень ВТСС ОИ ИСПДн КБ

№	Тип	Модель	Заводской номер	Расположение
1.	Телефон	Panasonic	FG4245-2233	Кабинет 226
2.	Телефон	Panasonic	FH3215-3421	Кабинет 226
3.	Кондиционер	Voxtel Prof 7250 W	0508044652	Кабинет 226
4.	Датчик пожарный	ИП-11	659493-59493-32	Кабинет 226
5.	Датчик пожарный	ИП-11	659493-59493-33	Кабинет 226
6.	Датчик пожарный	ИП-11	659493-59493-34	Кабинет 226
7.	Датчик охранный магнитоконтактный	б/н	инв. № 2011.23	Кабинет 226
8.	Датчик охранный магнитоконтактный	б/н	инв. № 2011.24	Кабинет 226
9.	Настольная лампа	б/н	инв. № 2011	Кабинет 226

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

Продолжение приложения Г

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

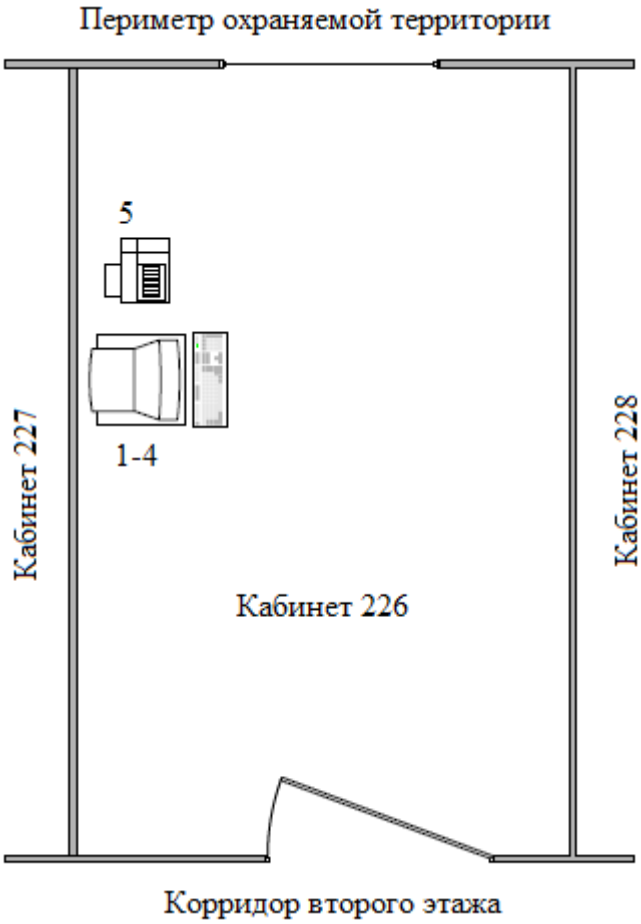

Рисунок 1 – Размещение ОТСС ИСПДн КБ.

*Примечание: Обозначения приведены в Таблице 2 основной части технического паспорта.

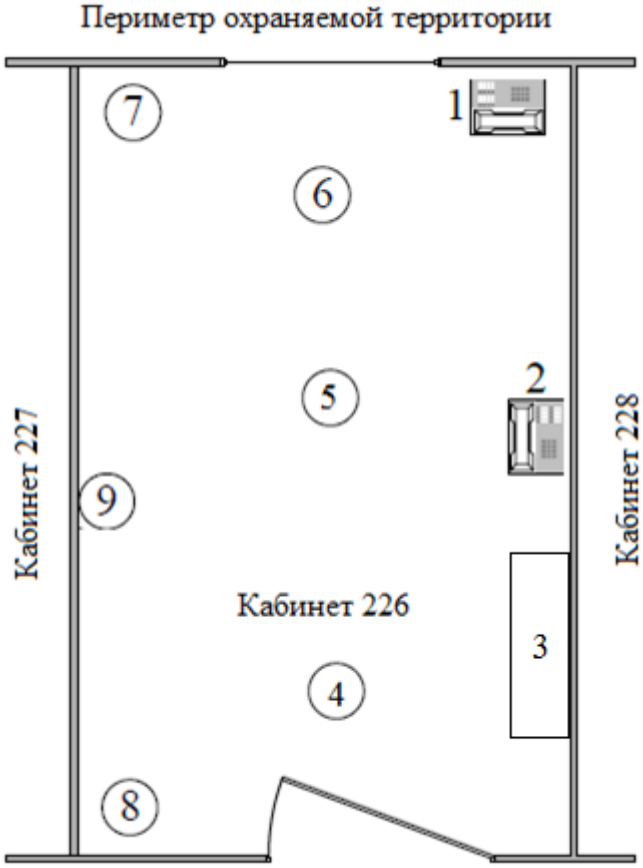

Рисунок 2.2 – Размещение ВТСС ИСПДн КБ.

*Примечание: Обозначения приведены в Таблице 2 основной части технического паспорта.

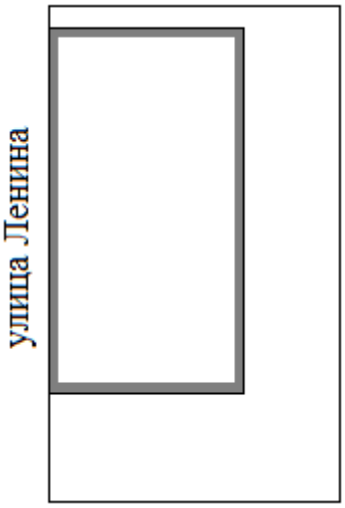

Рисунок 3 – Границы контролируемой зоны.

Продолжение приложения Г

Контролируемой зоной является огороженная территория УИТ государственного предприятия. Граница контролируемой зоны определена приказом «Об определении границ контролируемой зоны…».

Минимальное расстояние от ОТСС до КЗ составляет 10 метров.

Размещение ВТСС, линий приведено на рисунке 4.

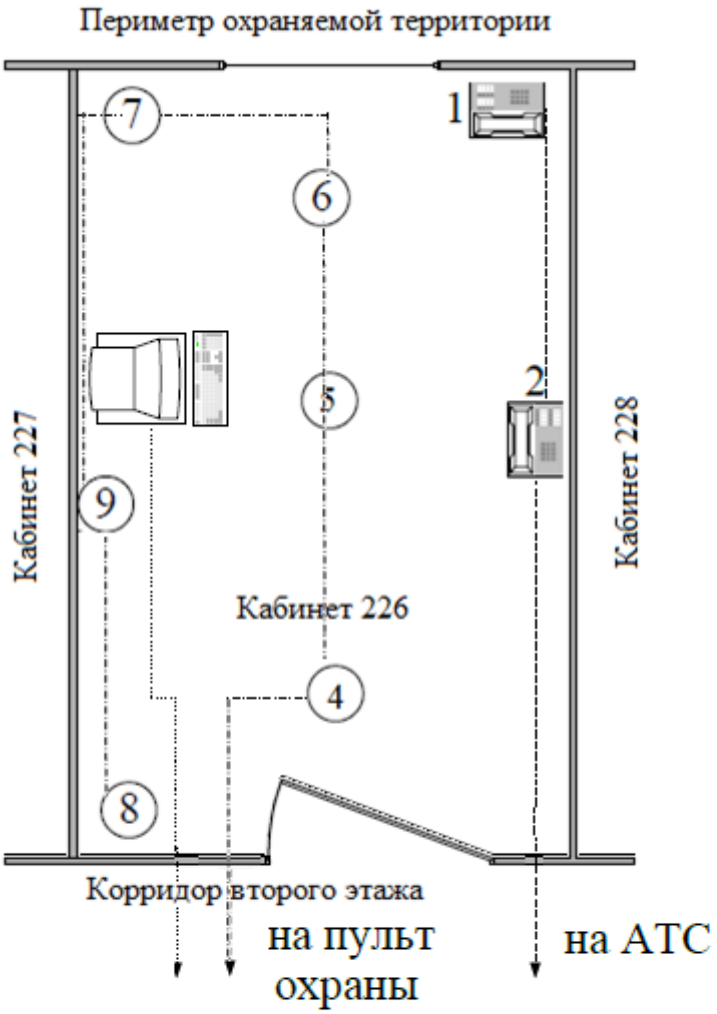

Рисунок 4 – Размещение ВТСС, расположение линий

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

Продолжение приложения Г

Размещение системы электропитания, заземления и инженерных коммуникаций приведено на рисунке 5.

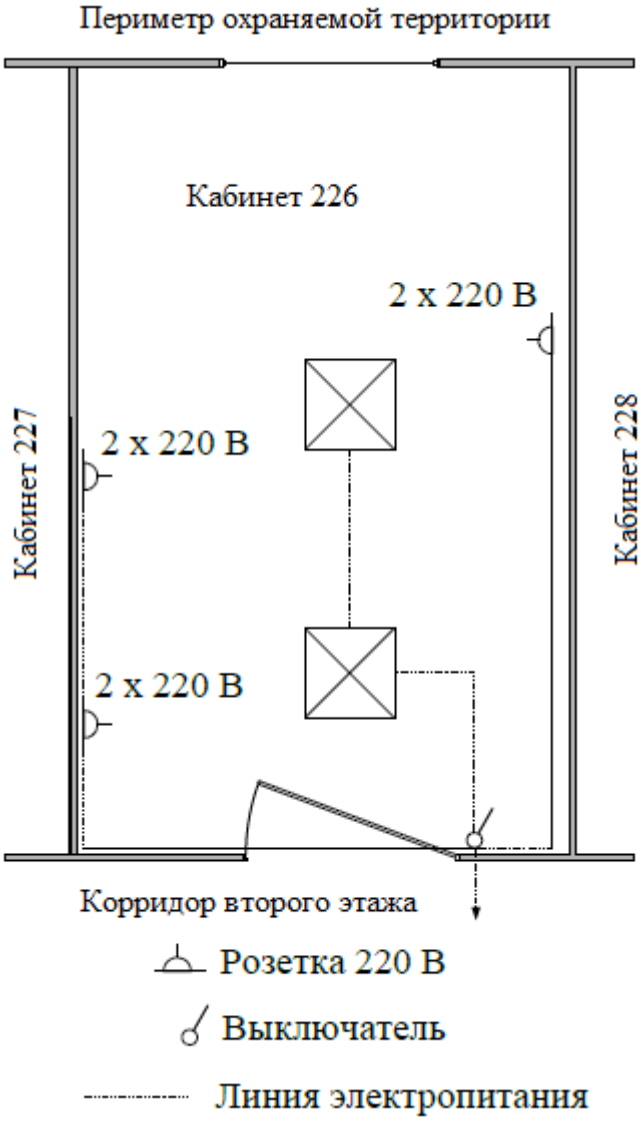

Рисунок 5 – Размещение системы электропитания, заземления и инженерных коммуникаций.

Линии электропитания, заземления, охранной и пожарной сигнализации, телефонной связи, отопления и ЛВС за пределы КЗ не выходят.

Продолжение приложения Г

Перечень средств защиты информации, установленных на объекте информатизации приведен в Таблице 3.

Таблица 3 - Перечень средств защиты

№	Наименование	Сертификат
1.	Операционная система Microsoft Windows 7 Профессиональная	Сертификат ФСТЭК № 2180/1 от 04.10.2011 (Действителен до 04.10.2020)
2.	Межсетевой экран Cisco ASA 5540	Сертификат ФСТЭК № 3677 от 30.11.2016 (Действителен до 30.11.2019)
3.	Программа антивирусной защиты Kaspersky Endpoint Security 10	Сертификат ФСТЭК № 3025 от 25.11.2013 (Действителен до 25.11.2019)

Продолжение приложения Г

Сведения о соответствии ОТСС объекта вычислительной техники требованиям по безопасности информации.

Протоколы испытаний и даты их регистраций.

_____

_____

_____

_____

_____

Сведения об аттестации объекта информатизации на соответствие требованиям по безопасности информации.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Окончание приложения Г

ПРИЛОЖЕНИЕ Д

ГОСУДАРСТВЕННОЕ ПРЕДПРИЯТИЕ

УТВЕРЖДАЮ

Заместитель генерального
директора по безопасности

_____ С.В. Перфилов

____ . _____ . 2018

Информационная система персональных данных клиент-банка
Частная модель угроз безопасности информации

Начальник службы безопасности

_____ В.А. Кашуба

____ . _____ . 2018

2018

Продолжение приложения Д

Таблица 1 - Частная модель угроз безопасности информации в «ИСПДн КБ».

	Наименование угрозы	Y_2	Y	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	Наименование угрозы
	Угрозы от утечки по техническим каналам						
I.	**Угрозы утечки видовой информации**						
1.	Просмотр информации на дисплее сотрудниками, не допущенными к обработке персональных данных	Малая	Низкая	Высокая	Актуальная		Инструкция пользователя Размещение дисплеев, исключающее несанкционированный просмотр
2.	Просмотр информации на дисплее посторонними лицами, находящимися в помещении в котором ведется обработка персональных данных	Малая	Низкая	Высокая	Актуальная		Инструкция пользователя Размещение дисплеев, исключающее несанкционированный просмотр
3.	Просмотр информации на дисплее посторонними лицами, находящимися за пределами помещения в котором ведется обработка персональных данных	Малая	Низкая	Высокая	Актуальная	Жалюзи на окнах	Инструкция пользователя
II.	**Угрозы утечки информации по каналам ПЭМИН**						
1.	Утечка информации по каналам ПЭМИН (сети электропитания, тех средства и пр.)	Малая	Низкая	Низкая	Неактуальная		Большая удаленность от границ КЗ
	Угрозы несанкционированного доступа к информации						

Продолжение таблицы 1

III.	**Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн**						
1.	Хищение ПЭВМ	Низкая	Средняя	Низкая	Неактуальная	Контроль пользователем при обработке информации во время работ	Инструкция пользователя
2.	Хищение съемных накопителей	Малая	Низкая	Высокая	Актуальная	Охранная сигнализация в помещении, где хранится сейф Контроль пользователем при обработке информации во время работ	Хранение в сейфе
3.	Кража ключей доступа/паролей	Малая	Низкая	Низкая	Неактуальная	Хранение в сейфе	Инструкция пользователя, администратора
4.	Модификация, уничтожение информации.	Низкая	Средняя	Высокая	Актуальная	Система защиты от НСД	Организация разграничения доступа
5.	Вывод из строя узлов ПЭВМ	Низкая	Средняя	Низкая	Неактуальная	В рабочее время контроль пользователем	
6.	Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	Низкая	Средняя	Высокая	Актуальная	Система защиты от НСД В рабочее время контроль пользователем	Ремонт специалистами УИТ, допущенными к обработке ПДн (согласно списка)
7.	Несанкционированное отключение средств защиты (САЗ и программных)	Малая	Низкая	Средняя	Неактуальная		Обеспечение возможности настройки СЗИ только администраторами Контроль доступа в помещение

							во время работы

Продолжение приложения Д

Продолжение таблицы 1

IV.	**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)**						
1.	Компьютерные вирусы	Низкая	Средняя	Низкая	Неактуальная	Антивирусное ПО, настройка СЗИ	Инструкция пользователя Инструкция администратора безопасности Регулярное обновление антивирусных баз
2.	Недекларированные возможности системного ПО и ПО для обработки персональных данных	Малая	Низкая	Низкая	Неактуальная	Доступ к исходным кодам имеют только разработчики Доступ к исполняемым файлам имеют администраторы	Организация разграничения доступа к исходным кодам и исполняемым модулям
3.	Установка ПО, не связанного с исполнением служебных обязанностей	Малая	Низкая	Низкая	Неактуальная	Настройка средств защиты операционной системы	Инструкция пользователя
4.	Внедрение аппаратных закладок	Малая	Низкая	Низкая	Неактуальная		Ремонт специалистами УИТ Инструкция обслуживающего персонала УИТ
V.	**Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и системы защиты ПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неатропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера**						
1.	Утрата ключей доступа/паролей	Низкая	Средняя	Низкая	Неактуальная	Съемные накопители информации большой емкости	Инструкция пользователя и АИБ Запрет записи паролей,

							хранение журналов с паролями администраторов в сейфе

Продолжение приложения Д

Продолжение таблицы 1

2.	Непреднамеренная модификация (уничтожение) информации сотрудниками	Низкая	Средняя	Высокая	Актуальная	Настройка средств защиты	
3.	Непреднамеренное отключение средств защиты, включая САЗ	Низкая	Средняя	Средняя	Актуальная	Доступ к установлению режимов работы средств защиты предоставляется только администратору безопасности Контроль пользователем во время работы	
4.	Выход из строя аппаратных средств (САЗ)	Низкая	Средняя	Средняя	Актуальная	Контроль пользователем во время работы Система сигнализации на САЗ	
5.	Сбой системы электроснабжения	Средняя	Средняя	Средняя	Актуальная	Использование источника бесперебойного электропитания	
6.	Стихийное бедствие (пожар)	Низкая	Средняя	Низкая	Неактуальная	Пожарная сигнализация на рабочем месте и в помещении, где расположен сейф	
VI.	**Угрозы преднамеренных действий внутренних нарушителей**						
	Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	Малая	Низкая	Высокая	Актуальная	Система защиты от НСД В нерабочее время съемный накопитель хранится в сейфе Контроль пользователем во время работы	Инструкция пользователя Контроль доступа в помещение ответственными сотрудниками

	Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	Низкая	Средняя	Высокая	Актуальная		Договоры с уполномоченными лицами

Окончание приложения Д

ПРИЛОЖЕНИЕ Е

ГОСУДАРСТВЕННОЕ ПРЕДПРИЯТИЕ

УТВЕРЖДАЮ

Заместитель генерального
директора по безопасности

_____ С.В. Перфилов

____ . _____ . 2018

ИНСТРУКЦИЯ

Типовая, технологическая администратора ИБ и ИС при работе в информационных системах, обрабатывающих конфиденциальную информацию

И-037-2018

Начальник службы безопасности

_____ В.А. Кашуба

____ . _____ . 2018

Начальник управления
информационных технологий

_____ В.Е. Кочетков

___ . _____ . 2018

2018

Продолжение приложения Е

1. Общие положения

1.1. Настоящая типовая инструкция определяет обязанности, права и ответственность администратора информационной безопасности и администратора информационной системы при работе в информационных системах, обрабатывающих конфиденциальную информацию.

1.2. Настоящей инструкцией должны руководствоваться в своей работе администраторы информационной безопасности и администраторы информационной системы, осуществляющие сопровождение информационных систем, обрабатывающих конфиденциальную.

1.3. Администраторы информационной безопасности и администраторы информационной системы, не ознакомленные с данной инструкцией, а также с изменениями и дополнениями к ней, к работе с информационной системы не допускаются.

1.4. К конфиденциальной информации относятся:

– служебная информация ограниченного распространения с пометкой «Для служебного пользования»;

– информация, составляющая коммерческую тайну;

– персональные данные.

1.5. Основными задачами администратора информационной безопасности для обеспечения безопасности конфиденциальной информации при её обработке являются:

- обеспечение защиты информации от нарушения ее конфиденциальности, целостности и доступности за счет несанкционированного доступа и воздействия;

- настройка, сопровождение и администрирование программных и аппаратных средств защиты информации;

- обеспечение защиты информации от воздействия вредоносного программного обеспечения;

Продолжение приложения Е

- определение и назначение прав и полномочий на доступ к защищаемым объектам доступа из принципа минимальной достаточности.

1.6. Основными задачами администратора информационной системы для обеспечения бесперебойной работы информационной системы, обрабатывающей конфиденциальную информацию, являются:

– установка, настройка и сопровождение всех программных средств, операционных систем и баз данных, входящих в состав информационной системы, за исключением средств защиты информации;

– оптимизация производительности программных средств, операционных систем и систем управления баз данных;

– резервное копирование обрабатываемой информации.

1.7. Администратор информационной безопасности имеет право доступа ко всем ресурсам информационной системы для обеспечения управления доступом пользователей к информации, обрабатываемой в информационной системе.

1.8. Все вносимые изменения в систему, которые напрямую или косвенно могут повлиять на процесс обработки информации, должны быть согласованы с администратором информационной безопасности.

1.9. Допускается совмещение функций администратора информационной безопасности с функциями администратора информационной системы.

1.10. Если в информационной системе не назначен администратор информационной безопасности, тогда функции администратора информационной безопасности, описанные в данной инструкции, выполняет администратор информационной системы.

1.11. Администратор информационной безопасности и/или администратор информационной системы (при необходимости) устанавливает и устраняет самостоятельно, либо совместно с техническим обслуживающим персоналом причины, ограничивающие производительность информационной системы.

Продолжение приложения Е

1.12. При выполнении своих обязанностей администратор информационной безопасности и администратор информационной системы руководствуются также:

– должностной инструкцией;

– эксплуатационной документацией на информационную систему;

– приказами и распоряжениями непосредственного руководителя;

– приказами и распоряжениями по предприятию;

– приказами и распоряжениями государственной корпорации по атомной энергии «Росатом»;

– стандартами предприятия;

– инструкциями по организации пропускного режима в помещения информационной системы;

– инструкциями по технике безопасности и пожарной безопасности;

– действующим законодательством Российской Федерации.

1.13. Администраторы информационной безопасности назначаются приказом заместителя генерального директора по безопасности.

1.14. Администраторы информационной системы назначаются приказом руководителя соответствующего структурного подразделения.

1.15. Администратором информационной безопасности может назначаться работник государственного унитарного предприятия (далее по тексту - предприятие), имеющий знания и навыки по администрированию и настройке программных и аппаратных средств защиты информации, используемых в информационной системе.

Администратор информационной безопасности должен периодически проходить подготовку в специализированных учебных центрах по программам, утвержденным уполномоченными в области обеспечения безопасности и технической защиты информации федеральными органами исполнительной власти, а

Продолжение приложения Е

также обучение порядку эксплуатации и администрированию применяемых в Госкорпорации «Росатом» средств защиты информации.

1.16. Администратором информационной системы может назначаться сотрудник предприятия, имеющий знания и навыки по администрированию программных средств (общесистемного и прикладного программного обеспечения), используемых в информационной системе.

1.17. Изменения и дополнения к данной инструкции утверждаются в установленном порядке.

2. Обязанности администраторов

2.1. Администраторы ИБ и ИС обязаны:

– знать общесистемное программное обеспечение и компьютерное оборудование, используемое в ИС;

– знать структуру служб каталогов Active Directory (в случае ее применения в ИС) и иметь навыки по ее администрированию;

– производить аудит журналов ОС, БД, прикладного ПО;

– предоставлять пользователям права доступа к ресурсам ИС по принципу минимальной достаточности;

– реагировать на сообщения от ответственных за обеспечение режима конфиденциальности и пользователей ИС о неисправностях в работе основных и вспомогательных средств, системного и прикладного ПО, а также СЗИ;

– немедленно ставить в известность персонал, осуществляющий техническое обслуживание, обо всех неисправностях аппаратных средств ИС;

– знать и выполнять требования эксплуатационной и организационно-распорядительной документации на ИС;

– знакомиться с действующими перечнями сведений, составляющих служебную информации ограниченного распространения, коммерческую тайну и

Продолжение приложения Е

– персональные данные в зависимости от уровня конфиденциальность информации, обрабатываемой в ИС;

– знать перечень информационных ресурсов, подлежащих защите на объекте информатизации;

– обеспечивать функционирование ИС в установленном штатном режиме;

– обеспечивать автоматический запуск антивирусного ПО при загрузке ОС (если не предусмотрен другой режим работы антивирусного ПО в ИС), при этом пользователь ИС не должен обладать возможностью его выгрузки;

– обновлять антивирусные базы не реже одного раза в месяц;

– немедленно реагировать на сообщение пользователя об обнаружении вирусов в ИС и принимать соответствующие меры;

– докладывать руководителю подразделения, ответственному за эксплуатацию объекта информатизации, о нарушениях или невыполнении пользователями ИС требований по защите конфиденциальной информации;

– проводить инструктаж и консультации пользователей ИС по правилам работы и эксплуатации средств вычислительной техники, а также своевременно оповещать об изменениях в регламенте и технологии обработки информации;

– делать необходимые отметки о выполнении работ в «Журнале учета работы и технического обслуживания ПЭВМ».

2.2. Администратор ИБ обязан:

В дополнение к обязанностям, указанным в п.3.1 настоящей инструкции.

– управлять учетными записями пользователей и доступом к ресурсам ИС;

– устанавливать и настраивать СЗИ от НСД в соответствии с требованиями, предъявляемыми к классу защищенности ИС;

– контролировать целостность программной среды;

– производить аудит журналов безопасности ОС и СЗИ от НСД;

– анализировать состояние системы ИБ, выявлять возможные каналы НСД к информации и готовить предложения по их устранению (предупреждению);

Продолжение приложения Е

– предотвращать использование, хранение и установку в ИС программ, не входящих в формуляр версии ПО и ИО, непосредственно не связанных с производственной деятельностью (игры и т.п.);

– организовать смену паролей пользователей в ОС (домене) не реже одного раза в год (если не определена другая периодичность локальной инструкцией на ИС);

– обеспечивать недоступность настроек СЗИ от НСД для пользователей;

– в случае компрометации идентификационных и аутентификационных данных (имени и пароля) пользователя, немедленно изменить их и проконтролировать соответствие установленных прав пользователей утвержденному состоянию;

– разрабатывать и контролировать реализацию антивирусной политики;

– своевременно восстанавливать систему защиты информации после отказа технических средств или аварий;

– участвовать в разработке нормативно-методических документов по вопросам защиты информации при ее автоматизированной обработке;

– оформлять и вести (своевременно корректировать) формуляры версии ПО и ИО;

– участвовать и контролировать проведение аттестационных испытаний ИС;

– уведомлять вышестоящее руководство о возникших угрозах информационной безопасности;

– проводить инструктаж и консультации пользователей ИС по требованиям защиты информации;

– принимать участие в работах по очистке жесткого магнитного диска (в случае необходимости) при сдаче на уничтожение или хранение, а также передаче в другую ИС;

Продолжение приложения Е

– консультировать обслуживающий персонал по вопросам ведения технического паспорта информационной системы;

– взаимодействовать с персоналом, осуществляющим техническое обслуживание, по вопросам обеспечения правильной эксплуатации средств вычислительной техники ИС;

– участвовать в составе комиссии по служебным расследованиям, проводимым в случае обнаружения фактов или попыток НСД к конфиденциальной информации, обрабатываемой в ИС;

– контролировать ведение технического паспорта объекта информатизации.

2.3. Администратор ИС обязан:

В дополнение к обязанностям, указанным в п.3.1 настоящей инструкции.

– осуществлять мониторинг производительности на серверах, функционирующих в ИС;

– своевременно принимать меры по повышению работоспособности и производительности системы;

– выполнять настройку ОС и прочих программных средств, осуществляющих обработку информации в ИС;

– при необходимости обновлять программное обеспечение на основании технического решения;

– своевременно восстанавливать ОС после отказа технических средств, аварий или системных сбоев;

– уведомлять администратора ИБ о возникших угрозах информационной безопасности;

– осуществлять резервное копирование баз данных и прочей защищаемой информации.

Продолжение приложения Е

3. Права администраторов

3.1. Администраторы ИБ и ИС имеют право:

– требовать от пользователей ИС точного соблюдения установленной технологии обработки информации и выполнения инструкций по обеспечению безопасности и защиты информации;

– обращаться к непосредственному руководителю с предложением о приостановке обработки конфиденциальной информации в случае нарушения установленной технологии обработки информации или нарушении функционирования программных средств;

– немедленно прекращать работу пользователей, если существует угроза потери или повреждения данных в результате нарушения работы ИС;

– вносить предложения по совершенствованию организации работ и повышению их эффективности;

– получать от руководителей необходимые дополнительные разъяснения и указания по выполняемой работе;

– проходить обучение с периодичностью, установленной в соответствии с утвержденной руководящей документацией.

4. Ответственность администраторов

4.1. На администратора ИБ и ИС возлагается ответственность за:

– разглашение конфиденциальной информации, ставшей ему известной в результате выполнения работ;

– некачественное выполнение проводимых им работ по обеспечению работоспособности ИС, в рамках своих обязанностей;

– превышение полномочий;

– нарушение правил охраны труда, техники безопасности, пожарной безопасности;

Продолжение приложения Е

– нерациональное использование выделенных материальных и технических ресурсов;

– за нарушение требований действующих на предприятии организационно-распорядительных документов и настоящей инструкции.

5.Доступ администраторов к ресурсам информационной системы

5.1. Работа администратора ИБ и ИС с ресурсами системы допускается только после выполнения процедур идентификации и аутентификации средствами установленной системы защиты информации.

5.2. Во время ввода пароля на клавиатуре должна быть исключена возможность его просмотра другими лицами.

5.3. При утрате или подозрении на компрометацию аутентификационных данных администратор ИБ должен немедленно изменить свой пароль или пароль администратора ИС.

Окончание приложения Е

ПРИЛОЖЕНИЕ Ж

ГОСУДАРСТВЕННОЕ ПРЕДПРИЯТИЕ

УТВЕРЖДАЮ

Заместитель генерального
директора по безопасности

_____ С.В. Перфилов

____ . _____ . 2018

ИНСТРУКЦИЯ

Типовая, технологическая по обеспечению защиты при работе в информационных системах, обрабатывающих конфиденциальную информацию

И-046-2018

Начальник службы безопасности

Начальник управления
информационных технологий

_____ В.А. Кашуба _____ В.Е. Кочетков

____ . _____ . 2018 ___ . _____ . 2018

2018

Продолжение приложения Ж

1. Общие положения

1.1. Настоящая типовая инструкция определяет порядок и правила защиты, а также обязанности, права и ответственность пользователей при работе в информационных системах, обрабатывающих конфиденциальную информацию.

1.2. К конфиденциальной информации относятся:

– служебная информация ограниченного распространения с пометкой «Для служебного пользования»;

– информация, составляющая коммерческую тайну;

– персональные данные.

1.3. Данная инструкция разработана в соответствии с «Положением о вычислительных сетях предприятия» П-476-453, «Положением об информационно-вычислительной сети предприятия» П-466-242 и предназначена для работников государственного предприятия (далее по тексту - предприятие), осуществляющих обработку конфиденциальной информации.

1.4. Пользователи, не ознакомленные с данной инструкцией, с «Положением о вычислительных сетях предприятия» и с «Положением об информационно-вычислительной сети предприятия», к работе в информационной системе, обрабатывающей конфиденциальную информацию, не допускаются.

1.5. Изменения и дополнения к данной инструкции утверждаются в установленном порядке.

1.6. Настоящей инструкцией должны руководствоваться в своей работе пользователи информационной системы, обрабатывающих конфиденциальную информацию.

2.Обязанности пользователя

2.1. Пользователь ИС, обрабатывающей конфиденциальную информацию, обязан:

Продолжение приложения Ж

– использовать систему только по ее непосредственному назначению (производить только те работы, которые предусмотрены технологическим процессом на ИС);

– знакомиться с нормативной, организационно-распорядительной и эксплуатационной документацией, относящейся к ИС, и изменениям к ней;

– соблюдать требования обеспечения информационной безопасности при эксплуатации ИС, обрабатывающей конфиденциальную информацию;

– знакомиться с действующими перечнями сведений, составляющих служебную информации ограниченного распространения («Для служебного пользования»), коммерческую тайну и персональные данные в зависимости от уровня конфиденциальность информации, обрабатываемой пользователем ИС;

– выполнять требования по эксплуатации системы в соответствии с действующей эксплуатационной документацией;

– блокировать рабочую станцию во время своего отсутствия на рабочем месте;

– следить за исправностью используемых технических средств и своевременно оповещать ответственного за обеспечение режима конфиденциальности, а также ответственного за техническое обслуживание об обнаруженных проблемах (самостоятельно устранять возникшие неисправности, изменять состав технических средств запрещено);

– перед началом работы проверять целостность защитной пломбировочной наклейки (печати и/или специальных защитных знаков) на корпусе системного блока ПЭВМ. В случае нарушения целостности незамедлительно ставить в известность ответственного за обеспечение режима конфиденциальности и администратора ИБ;

– следить за тем, чтобы антивирусное ПО постоянно находилось в состоянии «Включено»;

Продолжение приложения Ж

– до начала использования отчуждаемого МНИ проверять его на наличие вирусов;

– незамедлительно сообщать ответственному за обеспечение режима конфиденциальности об утрате учтенного в установленном порядке носителя конфиденциальной информации (отчуждаемые МНИ);

– незамедлительно ставить в известность администратора ИБ в случае обнаружения попытки несанкционированного доступа к средствам вычислительной техники;

– оповещать администратора ИС в случае возникновения сбоев в работе и ОС и прикладного ПО;

– обеспечивать сохранность «Журнала учета работы и технического обслуживания ПЭВМ», в котором делаются отметки обо всех изменениях, связанных с ПЭВМ;

– обеспечивать сохранность используемых в работе носителей конфиденциальной информации.

2.2. Пользователю ИС запрещается:

– передавать свой пароль другим лицам и записывать его на чем-либо;

– обрабатывать конфиденциальную информацию, если существует вероятность её визуального просмотра посторонними лицами;

– оставлять носители (машинные, традиционные) конфиденциальной информации в условиях, при которых возможно нарушение конфиденциальности, целостности или доступности хранимой на них информации посторонними лицами;

– изменять программную среду рабочей станции, самостоятельно устанавливать какое-либо программное обеспечение (за исключением согласованного с администратором ИБ), изменять конфигурацию и настройки СЗИ, ОС;

– использовать идентификатор и пароль другого пользователя;

Продолжение приложения Ж

– пытаться изменить свои полномочия и привилегии в системе, удалять системные журналы ОС и журналы безопасности СЗИ;

– использовать недокументированные возможности и ошибки ПО;

– использовать в работе неучтенные (незарегистрированные) в установленном порядке носители информации (НЖМД и отчуждаемые МНИ);

– подключать к рабочим станциям и сети ИС постороннее оборудование, не задекларированное в техническом паспорте (сотовые телефоны, модемы, фотоаппараты и т.п.).

3. Права пользователя

3.1. Пользователь ИС, обрабатывающей конфиденциальную информацию, имеет право:

– требовать от своего непосредственного руководителя оборудования рабочего места в соответствии с требованиями санитарных правил и норм, а также требованиями нормативных документов по обеспечению защиты информации;

– использовать прикладные программы, обрабатывающие конфиденциальную информацию в ИС, для решения производственных задач;

– прекращать обработку конфиденциальной информации в ИС при возникновении проблем, которые могут привести к ее разглашению и/или порче;

– подавать предложения своему непосредственному руководителю по внесению изменений в существующую технологию обработки данных, а также – по модернизации специального ПО;

– в случае необходимости получать от ответственного за режим конфиденциальности информации или администратора ИС дополнительные разъяснения и указания по выполняемой работе.

Продолжение приложения Ж

4. Ответственность пользователя

4.1. Пользователь несет ответственность за нарушение требований действующих на предприятии организационно-распорядительных документов и настоящей инструкции, а также за:

– разглашение конфиденциальной информации, ставшей ему известной в результате выполнения работ, в том числе, значения пароля от персональной учетной записи;

– невыполнение требований информационной безопасности при функционировании ИС;

– нарушение целостности и комплектности технических и программных средств своей рабочей станции;

– нецелевое использование предоставленных ему для выполнения производственных функций технических средств обработки информации;

– несвоевременное оповещение ответственного за обеспечение режима конфиденциальности, администратора ИС, а также ответственного за техническое обслуживание о выявленных им проблемах эксплуатации ИС (неисправности, попытки несанкционированного доступа);

– утрату учтенных и предназначенных для хранения конфиденциальной информации НЖМД и отчуждаемых МНИ;

– нарушение правил охраны труда, техники безопасности, пожарной безопасности.

– невыполнение требований прочих действующих инструкций, указаний, распоряжений и нормативных документов по информационной безопасности.

5. Порядок выполнения технологических операций пользователем

5.1. Выполнение подготовительных действий к использованию ИС, обрабатывающей конфиденциальную информацию

Продолжение приложения Ж

5.1.1. Задача «Получение доступа к ИС»

5.1.1.1. Для получения доступа к ИС пользователь должен:

– быть ознакомленным под подпись с инструкциями, эксплуатационной и прочей документацией необходимой для осуществления корректной обработки информации с соблюдением режима безопасности конфиденциальной информации;

– пройти соответствующую подготовку по выполнению операций в прикладных задачах, обрабатывающих конфиденциальную информацию.

5.1.2. Задача «Подготовка к работе»

5.1.2.1. Перед использованием ИС пользователь должен:

– убедиться в целостности защитной пломбировочной наклейки (печати и/или специальных защитных знаков) на используемой рабочей станции;

– убедиться, что исключена возможность просмотра посторонними лицами отображаемой на экране монитора информации.

5.1.3. Задача «Вход в систему»

5.1.3.1. После включения рабочей станции и загрузки ОС, пользователю необходимо пройти процедуры аутентификации и идентификации, для чего после

полной загрузки ОС необходимо ввести в предложенном диалоге имя пользователя и пароль.

5.1.3.2. В случае если процедуру пройти не удается, необходимо об этом сообщить администратору ИС либо иным лицам, которым делегировано право по управлению паролями в ИС.

5.1.3.3. Набор пароля на клавиатуре должен выполняться так, чтобы исключить его просмотр другими лицами.

5.2. Выполнение действий по окончании использования ИС

5.2.1. Перед тем как отлучиться с рабочего места пользователь должен заблокировать рабочую станцию, используя комбинацию клавиш Ctrl+Alt+Del, или дождаться появления экранной заставки, защищенной паролем.

Продолжение приложения Ж

5.2.2. По окончании работы в ИС пользователь должен корректно завершить работу с программным обеспечением и выключить рабочую станцию («Пуск» – «Завершение работы» – «Выключить компьютер»).

5.2.3. Убрать в закрывающийся ящик или сейф, предназначенный для хранения конфиденциальных сведений, используемые в работе учтенные отчуждаемые МНИ.

Окончание приложения Ж

ПРИЛОЖЕНИЕ З

ГОСУДАРСТВЕННОЕ ПРЕДПРИЯТИЕ

УТВЕРЖДАЮ

Заместитель генерального
директора по безопасности

_____ С.В. Перфилов

____ . _____ . 2018

ИНСТРУКЦИЯ

Типовая, технологическая, для технического обслуживающего персонала информационных систем, обрабатывающих конфиденциальную информацию

И-029-2018

Начальник службы безопасности	Начальник управления информационных технологий
_____ В.А. Кашуба	_____ В.Е. Кочетков
____ . _____ . 2018	___ . _____ . 2018

2018

Продолжение приложения З

1. Общие положения

1.1. Настоящая инструкция разработана для персонала отдела технического обслуживания управления информационных технологий государственного предприятия. Инструкция определяет требования к информационной безопасности, обязанности, права и ответственность технического обслуживающего персонала при проведении ремонта и технического обслуживания оборудования информационных систем по обработке конфиденциальной информации - служебной информации ограниченного распространения, не составляющей государственную тайну.

1.2. Субъектами доступа к ресурсам ИС являются:

– пользователи ИС;

– администраторы ИС;

– администраторы информационной безопасности (АИБ);

– технический обслуживающий персонал.

1.3. Все находящиеся в обращении несъемные жесткие магнитные диски (НЖМД) компьютеров на предприятии, на которых обрабатывается конфиденциальная информация, подлежат учёту в соответствии с инструкцией

«Порядок учета и обращения с несъемными жесткими магнитными дисками компьютеров, обрабатывающих конфиденциальную информацию».

1.4. Технический обслуживающий персонал осуществляет техническую эксплуатацию основных технических средств и систем, обрабатывающих конфиденциальную информацию, выполняет плановые и внеплановые работы по обеспечению работоспособности ИС.

1.5. Методическое руководство по информационной безопасности объекта информатизации осуществляют АИБ.

1.6. Технический обслуживающий персонал имеет право вносить предложения по изменению и дополнению данной инструкции.

Продолжение приложения З

1.7. Технический обслуживающий персонал, не ознакомленный с данной инструкцией к работе в ИС, обрабатывающей конфиденциальную информацию, не допускается.

1.8. Изменения и дополнения к данной инструкции утверждаются в установленном порядке.

1.9. Настоящей инструкцией должны руководствоваться в своей работе технический обслуживающий персонал ИС, обрабатывающих конфиденциальную информацию.

2. Обязанности технического обслуживающего персонала

2.1. Технический обслуживающий персонал обязан:

– ознакомиться с данной инструкцией. Работники, не ознакомленные с настоящей инструкцией, а также с изменениями и дополнениями к ней, к техническому обслуживанию технических средств в ИС не допускаются.

– выполнять требования по обслуживанию ИС в соответствии с действующей эксплуатационной документацией;

– периодически производить профилактические работы и комплексную проверку работоспособности технических средств ИС.

– своевременно реагировать на сообщения администраторов ИС, АИБ и пользователей ИС о любых неисправностях в работе технических средств;

– незамедлительно ставить в известность АИБ в случае обнаружения попытки несанкционированного доступа к конфиденциальной информации или при обнаружении компьютерных вирусов;

– перед проведением ремонтных или профилактических работ проверять целостность защитной пломбировочной наклейки (печати и/или специальных защитных знаков) на корпусе ПЭВМ. В случае нарушения целостности незамедлительно ставить в известность АИБ;

Продолжение приложения З

– при каждом обслуживании ПЭВМ делать отметки о выполняемых работах а также обо всех изменения, связанных с ПЭВМ в «Журнале учета работы и технического обслуживания ПЭВМ»;

– обеспечивать сохранность учтенных НЖМД при проведении ремонтных работ;

– соблюдать требования обеспечения информационной безопасности при выполнении работ в ИС, обрабатывающей конфиденциальную информацию.

3. Доступ к аппаратным ресурсам информационной системы

3.1. Под аппаратными ресурсами следует понимать основные технические средства и системы, указанные в техническом паспорте на ИС.

3.2. Обязательными условиями получения доступа к ресурсам ИС технического обслуживающего персонала являются:

– приказ о назначении технического обслуживающего персонала ИС, утвержденный заместителем генерального директора по безопасности – начальником управления безопасности;

– знание технологии обработки информации в ИС с учетом требований информационной безопасности.

3.3. Технический обслуживающий персонал не имеет права производить замену учтенного НЖМД ПЭВМ без утвержденного технического решения, согласованного с СБГП.

4. Порядок работы обслуживающего персонала

В соответствии с инструкцией И-025-2018 на корпусе каждой ПЭВМ, входящей в состав ИС, должна быть нанесена защитная пломбировочная наклейка, предотвращающая вскрытие корпуса без повреждения наклейки.

На каждый НЖМД из состава ИС должна быть нанесена пломбировочная наклейка с уникальным номером. В случае с моноблоком пломбировочная наклейка с уникальным номером наносится на корпус моноблока.

Номер, указанный на пломбировочной наклейке используется как уникальный учётный номер НЖМД.

На корпус каждой ПЭВМ, входящей в состав ИС, должна быть наклеена этикетка.

4.1. Перед проведением технического обслуживания технический обслуживающий персонал проверяет целостность защитной пломбировочной наклейки на корпусе ПЭВМ. В случае её повреждения либо отсутствия технический обслуживающий персонал сообщает об этом АИБ. Дальнейшими действиями обслуживающего персонала методически руководят АИБ.

4.2. При включении в состав ИС новой ПЭВМ, по утвержденному техническому решению, технический обслуживающий персонал выполняет следующие действия:

– производит вскрытие корпуса ПЭВМ;

– наклеивает пломбировочную наклейку с уникальным номером на НЖМД;

– наклеивает этикетку с учётным номером НЖМД на корпус ПЭВМ;

– после закрытия корпуса ПЭВМ производит его опечатывание защитной пломбировочной наклейкой, в которую вписывает свою фамилию, инициалы и ставит подпись;

– записывает в «Журнал учёта работ и технического обслуживания ПЭВМ» данные о проведенной работе, учетный номер НЖМД, номер защитной пломбировочной наклейки, свою фамилию, инициалы, ставит подпись;

– информирует ответственного за учёт и АИБ о новом учётном номере НЖМД.

Продолжение приложения З

4.3. Технический обслуживающий персонал выполняет техническое обслуживание ПЭВМ согласно утвержденному графику ППР, а также по заявке пользователей.

4.3.1. При необходимости вскрытия ПЭВМ технический обслуживающий персонал выполняет следующие действия:

– отклеивает защитную пломбировочную наклейку (индикация вмешательства) с ПЭВМ и вклеивает её в «Журнал учёта работ и технического обслуживания ПЭВМ»;

– производит вскрытие корпуса ПЭВМ и выполняет необходимые работы;

– после закрытия корпуса ПЭВМ производит его опечатывание новой защитной пломбировочной наклейкой, в которую вписывает свою фамилию, инициалы и ставит подпись;

– записывает в «Журнал учёта работ и технического обслуживания ПЭВМ» данные о проведенной работе, номер новой защитной пломбировочной наклейки, свою фамилию, инициалы, ставит подпись.

4.3.2. При необходимости замены ПЭВМ из состава ИС технический обслуживающий персонал готовит техническое решение и согласует с СБГП.

При замене технический обслуживающий персонал выполняет следующие действия:

– производит вскрытие корпуса новой ПЭВМ;

– наклеивает пломбировочную наклейку с уникальным номером на НЖМД;

– наклеивает этикетку с учётным номером НЖМД на корпус новой ПЭВМ, либо заменяет старую этикетку;

– после закрытия корпуса ПЭВМ производит его опечатывание новой защитной пломбировочной наклейкой, в которую вписывает дату оклеивание, свою фамилию, инициалы и ставит подпись;

Продолжение приложения З

– записывает в «Журнал учёта работ и технического обслуживания ПЭВМ» данные о проведенной работе, учетный номер нового НЖМД, номер новой защитной пломбировочной наклейки, свою фамилию, инициалы, ставит подпись;

– информирует ответственного за учёт в данном структурном подразделении и АИБ об изменении учетного номера НЖМД;

– после замены старый НЖМД передается на склад УИТ.

Удаление информации с НЖМД и составление акта стирания конфиденциальной информации с НЖМД выполняют АИБ.

Уничтожение НЖМД и составление акта уничтожения НЖМД выполняет технический обслуживающий персонал.

5. Контроль

5.1. Факт проведения работ отражается в «Журнале учета работы и технического обслуживания ПЭВМ».

5.2. Контроль за ведением «Журнала учета работы и технического обслуживания ПЭВМ» возлагается на руководителей групп отдела технического обслуживания.

5.3. Контроль выполнения всех вышеизложенных требований возлагается на начальника УИТ.

5.4. Контроль целостности защитной пломбировочной наклейки выполняет технический обслуживающий персонал во время проведения технического обслуживания до начала выполнения работ.

6.Ответственность

6.1. Технический обслуживающий персонал несет ответственность за:

– нарушение требований действующих на предприятии организационно-распорядительных документов и настоящей инструкции;

Продолжение приложения З

– разглашение сведений конфиденциального характера, ставших им известными при выполнении своих служебных обязанностей;

– несвоевременное оповещение ответственного за конфиденциальность АИБ о выявленных им проблемах эксплуатации ИС;

– невыполнение требований информационной безопасности при функционировании ИС;

– невыполнение требований действующих инструкций, указаний, распоряжений и нормативных документов по информационной безопасности;

– невыполнение обязанностей, определенных настоящей инструкцией;

– небрежное хранение учтенных НЖМД и отчуждаемых машинных носителей информации, входящих в состав ИС, изъятых для ремонта;

– некачественное выполнение работ;

– неправомерное использование ресурсов ИС;

– нарушение правил охраны труда, техники безопасности, пожарной безопасности.

6.2. За ненадлежащее выполнение своих служебных обязанностей технический обслуживающий персонал несет административную и уголовную ответственность в соответствии с действующим законодательством Российской Федерации.

7. Права

7.1. Технический обслуживающий персонал имеет право:

– требовать от своего непосредственного руководителя оборудования рабочего места в соответствии с требованиями санитарных правил и норм, а также требованиями режима конфиденциальности;

– использовать прикладные программы, обрабатывающие конфиденциальную информацию в ИС, для решения производственных задач;

Продолжение приложения З

– подавать предложения своему непосредственному руководителю по внесению изменений в существующую технологию обработки данных, а также – по модернизации специального ПО;

– получать от АИБ дополнительные разъяснения и указания по выполняемой работе.

Окончание приложения З

ПРИЛОЖЕНИЕ И

ГОСУДАРСТВЕННОЕ ПРЕДПРИЯТИЕ

УТВЕРЖДАЮ

Заместитель генерального
директора по безопасности

_____ С.В. Перфилов

____ . _____ . 2018

Информационная система персональных данных клиент-банка

Программа и методики проведения аттестационных испытаний
«Информационной системы персональных данных клиент-банка»

№ 30/95 ДС

2018

Продолжение приложения И

1.Общие положения

Настоящий документ определяет цели, задачи, методы, условия, объем, порядок и методики проведения аттестационных испытаний информационной системы персональных данных клиент-банка (далее ИСПДн КБ) на соответствие требованиям по обеспечению безопасности персональных данных.

Состав ОТСС приведен в таблице 1.

Таблица 1 – состав ОТСС.

№	Наименование устройства	Модель	Заводской номер
1.	Системный блок	IRU Brava Home 114W	10157
2.	Монитор	Samsung S27A750D	ETL460C260723157E
3.	Клавиатура	Genius KM-122	ZM6C02019509
4.	Мышь	A4Tech X7 XL-750BX	130-130009-200
5.	МФУ	Samsung SCX-4100	CNKDS08892

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».

Задачей аттестационных испытаний является оценка защищенности ИСПДн 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

Продолжение приложения И

информационного обмена (электромагнитное, через специально внедренные программные средства («закладки»);

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.

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.

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.

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.

Объектом аттестационных испытаний является ИСПДн КБ УИТ государственного предприятия, уровня защищенности «4», размещенная по адресу: г. Озерск, ул. Герцена, д. 7, кабинет № 226.

Продолжение приложения И

Перечень программных средств, с помощью которых проводится проверка выполнения требований по безопасности информации на объекте информатизации представлен в таблице 2.

Таблица 1.2 – Перечень инструментальных средств.

Тип средства измерений	Наименование	Заводской номер	Дата проверки
Программа фиксации и контроля исходного состояния программного комплекса	«ФИКС» (версия 2.0.1)	№ А 267757	Сертификат ФСТЭК № 913, действ. до 01.06.2019 г.

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

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.

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;

Продолжение приложения И

– устранение установленных недостатков и нарушений, в согласованные с комиссией сроки, с представлением необходимых документов в УИТ государственного предприятия;

– проведение дополнительных испытаний по дополнительному соглашению;

– применение дополнительных организационно-технических мер защиты.

«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.

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.

Проверка правильности определения уровня защищенности объекта информатизации:

– проверка ПДн, циркулирующих в ИСПДн, для проверки правильности определения уровня защищенности ИСПДн;

– проверка уровня полномочий субъектов доступа к ИСПДн;

– проверка режимов обработки информации.

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

Продолжение приложения И

– 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.

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

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

Подготовка отчетной документации и оценка результатов испытаний аттестуемого объекта.

Результаты аттестационных испытаний оформляются протоколом испытаний, содержащим:

– состав комиссии, дату испытаний, наименование аттестуемого объекта;

– цель испытаний;

– перечень нормативных документов и методик испытаний;

– результаты испытаний.

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».

Продолжение приложения И

3. Методика аттестационных испытаний информационной системы на соответствие требованиям по безопасности информации

Общие положения.

Настоящая методика предназначена для проведения аттестационных испытаний ИСПДн КБ УИТ государственного предприятия, уровня защищенности «4», размещенной по адресу: Челябинская обл., г. Озерск, ул. Герцена, д. 7, кабинет № 226 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 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.

Проведение испытаний.

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;

Продолжение приложения И

– акт классификации 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 пользователей 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.

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

Продолжение приложения И

При исследовании технологического процесса информационной системы 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.

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.

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

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

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

По результатам исследований уточняется схема технологического процесса отдельных средств обработки и передачи информации.

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

Продолжение приложения И

Проверка ИСПДн на соответствие организационно-техническим требованиям по защите информации проводится в объеме, указанном в таблице 3.

Таблица 3 – Объем работ.

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
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

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.

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 информационную систему, а также возможных критических мест информационной системы, снижающих уровень защиты.

Продолжение приложения И

Анализируются средства и системы защиты информации, устраняющие выявленные опасные факторы и угрозы.

Проверка правильности присвоения уровня защищенности ИСПДн производится в соответствии с требованиями постановления Правительства

Российской Федерации от 1 ноября 2012 г. № 1119. Полученный уровень защищенности ИСПДн сравнивается с установленным на объекте информатизации.

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.

Производится проверка наличия 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.

Производится проверка выполнения требований руководящих документов по условиям размещения технических средств в помещениях, которые исключали

Продолжение приложения И

бы возможность несанкционированного просмотра информации с экранов мониторов, с распечаток принтеров и с других устройств ввода-вывода информации.

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

Проверка ИСПДн на соответствие требованиям по защите информации.

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 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 ИСПДн.

Под штатными средствами доступа к информации на ПЭВМ 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 ПЭВМ, снижающих уровень защиты; проверка наличия документов по разрешительной системе доступа персонала к защищаемой информации, хранящейся и (или) обрабатываемой в ПЭВМ;

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

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

Проверка подсистемы идентификации и аутентификации субъектов доступа и объектов доступа.

Проверка настройки управления доступом субъектов доступа к объектам доступа.

Проверка параметров настройки ограничения программной среды.

Проверка процесса защиты машинных носителей информации, на которых хранятся и обрабатываются персональные данные.

Проверка регистрации событий безопасности.

Проверка реализации антивирусной защиты.

Проверка реализации средств обнаружения вторжений.

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

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.

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 рабочей станции ИСПДн.

Реализация требований по обеспечению доступности персональных данных:

– проверка резервного копирования ПДн;

– проверка возможности восстановления ПДн с резервных машинных носителей.

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.

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

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 выявление инцидентов и реагирования на них;

– проверка обнаружения, идентификации и регистрации инцидентов;

– проверка принятия мер по устранению инцидентов.

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.

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 Приказа 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 ПДн».

Перечень организационно-распорядительных и нормативных документов, на соответствие которым проводятся аттестационные испытания объекта информатизации:

– федеральный закон Российской Федерации от 27 июля 2006 г. 152-ФЗ «О персональных данных»;

– «Постановление об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1 ноября 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»;

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

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

– 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.);

– 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);

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

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

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

Руководитель аттестационной комиссии

В.А. Кашуба

«_____»_____2018 г.

ПРИЛОЖЕНИЕ К

ГОСУДАРСТВЕННОЕ ПРЕДПРИЯТИЕ

УТВЕРЖДАЮ

Заместитель генерального
директора по безопасности

_____ С.В. Перфилов

____ . _____ . 2018

ПРОТОКОЛ

аттестационных испытаний объекта информатизации
«Информационной системы персональных данных клиент-банка»
на соответствие организационным требованиям по защите информации

№ 789/12

Начальник службы безопасности

_____ В.А. Кашуба

____ . _____ . 2018

Продолжение приложения К

1.Состав комиссии, дата испытаний, наименование аттестуемого объекта

Аттестационная комиссия в составе: М.А. Арасланов, М.О. Бушуев, Д.С. Силантьев провела аттестационные испытания объекта информатизации «Информационная система персональных данных клиент-банка» («ИСПДн КБ») в соответствии с требованиями нормативных и методических документов ФСТЭК России по аттестации объектов информатизации по требованиям безопасности информации.

2.Краткое описание аттестуемого объекта и цель испытаний

«ИСПДн КБ» реализована на базе персональной электронно-вычислительной машины (ПЭВМ), имеющей выход в сеть Интернет, размещённой в помещении 226 по улице Герцена, д. 7.

Состав основных технических средств и систем (ОТСС) «ИСПДн КБ» представлен в таблице 1.

Таблица 1 – Состав ОТСС «ИСПДн КБ»

№	Наименование устройства	Модель	Заводской номер
1.	Системный блок	IRU Brava Home 114W	10157
2.	Монитор	Samsung S27A750D	ETL460C260723157E
3.	Клавиатура	Genius KM-122	ZM6C02019509
4.	Мышь	A4Tech X7 XL-750BX	130-130009-200
5.	МФУ	Samsung SCX-4100	CNKDS08892

«ИСПДн КБ» предназначена для приёма и передачи документов (платёжных, зарплатных реестров и т.п.) в банки, где открыты расчетные счета государственного предприятия.

Уровень защищённости персональных данных – 4.

Целью испытаний является оценка соответствия принятых организационно-технических мер по обеспечению безопасности конфиденциальной информации в соответствии с действующими требованиями нормативно-правовых документов по защите информации.

Аттестация проводится в соответствии с «Положением по аттестации объектов информатизации по требованиям безопасности информации», утвержденным председателем Гостехкомиссии России 25 ноября 1994 г.

3.Перечень нормативных документов и методик испытаний

Аттестационные испытания объекта информатизации проводились в соответствии с документом «Программа и методики проведения аттестационных испытаний информационной системы персональных данных клиент-банка (ИСПДн КБ)» (далее «Программа и методики…»).

Перечень организационно-распорядительных и нормативных документов, на соответствие которым проводились аттестационные испытания:

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

– указ Президента Российской Федерации «Об утверждении перечня сведений конфиденциального характера» от 06.03.97 № 188;

– постановление Правительства Российской Федерации «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии» от 03.11.94 № 1233;

– «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К), утвержденные приказом Государственной технической комиссии при Президенте РФ от 03.08.2002 № 282;

– руководящий документ Гостехкомиссии России «Защита от НСД к информации. Термины и определения»;

– руководящий документ Гостехкомиссии России «Концепция защиты средств вычислительной техники и автоматизированных систем от НСД»;

– руководящий документ Гостехкомиссии России «Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации»;

– руководящий документ Гостехкомиссии России «Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности информации»;

– руководящий документ Гостехкомиссии России «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники»;

– руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей»;

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

– постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденные приказом Федеральной службой по техническому и экспортному контролю России от 18.02.2013 № 21;

– положение «О телекоммуникационном узле государственного предприятия для связи с сетью Интернет»;

– положение «Порядок работы пользователя абонентского пункта с сетью интернет»;

– ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на

автоматизированные системы. Автоматизированные системы. Термины и определения»;

– ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»;

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

– ГОСТ 34.603-92 «Информационная технология. Виды испытаний автоматизированных систем»;

– ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования»;

– 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 РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения»;

– «Порядок регистрации, обращения, хранения и уничтожения документов и машинных носителей информации, содержащих служебную информацию ограниченного распространения, в государственном предприятии И-037-2016;

– Инструкция «Порядок учета и обращения с несъемными жесткими магнитными дисками компьютеров, обрабатывающих конфиденциальную информацию»

4. Результаты испытаний

4.1. Объем проводимых аттестационных испытаний объекта информатизации на соответствие организационным требованиям по защите информации

Испытания проводились в объеме, предусмотренном разделом 3 «Программы и методик…», и включали в свой состав:

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

– проверку соответствия состава и структуры программно-технических средств «ИСПДн КБ» представленной документации;

– проверку правильности классификации «ИСПДн КБ»;

– проверку уровня подготовки кадров и распределения ответственности персонала;

– проверку наличия сертификатов соответствия на средства защиты информации;

– проверку достаточности принятых организационных мер по ограничению доступа к техническим средствам «ИСПДн КБ».

При проведении аттестационных испытаний применялся экспертно-документальный метод, предусматривающий проверку соответствия «ИСПДн КБ» требованиям по безопасности информации на основании экспертной оценки полноты и достаточности представленных документов по обеспечению необходимых мер защиты информации в «ИСПДн КБ», а также соответствия реальных условий эксплуатации требованиям по размещению, монтажу и эксплуатации «ИСПДн КБ».

4.2 Проверка достаточности представленных документов и соответствия их содержания требованиям по безопасности информации

В ходе подготовки и проведения проверки комиссии были представлены документы, приведенные в таблице 2.

Продолжение приложения К

Таблица 2 – Представленные документы

№	Наименование документа	Номер документа
1.	Техническое задание на создание системы защиты информации в ИС	ЕЕ.338758.В20 1В
2.	Описание технологического процесса обработки информации	ЕЕ.338754.В20 РА
3.	Технический паспорт ИС	ЕЕ.14082.К58 КЭ
4.	Акт классификации ИС	4.2.1./1915
5.	Инструкция типовая, технологическая по обеспечению защиты конфиденциальной информации	И-046-2018
6.	Инструкция типовая, технологическая администратора ИБ и АС	И-037-2018
7.	Инструкция типовая, технологическая для технического обслуживающего персонала	И-029-2018
8.	Приказ о создании комиссии для проведения аттестационных испытаний объекта информатизации	НН.3872 АК
9.	Приказ о назначении пользователей, ответственных за обеспечение безопасности персональных данных	НН.2836 ЧС
10.	Акты обследований помещений на соответствие требованиям по защите персональных данных	543.43/548
11.	Заключение экспертной комиссии	47/4
12.	Перечень защищаемых ресурсов	324.43/1
13.	Список пользователей, допущенных до работы в ИС	4398.5 РО

Вывод: утверждена основная часть организационно-распорядительной документации на «ИСПДн КБ»;

4.3 Проверка соответствия состава и структуры программно-технических средств «ИСПДн КБ» представленной документации

Описание и состав объекта информатизации сформированы на основании предоставленных заявителем аттестационных испытаний исходных данных, а также по результатам предварительного ознакомления с объектом.

Состав, структура и размещение технических средств, реально установленных на объекте, соответствуют данным, представленным в техническом паспорте ЕЕ.14082.К58 КЭ.

Продолжение приложения К

Состав программного обеспечения, установленного в «ИСПДн КБ», соответствует представленному в техническом паспорте ЕЕ.14082.К58 КЭ.

Вывод: состав и структура программно-технических средств «ИСПДн КБ» соответствует представленной документации.

4.4 Проверка правильности классификации ИС

Классификация «ИСПДн КБ» проведена на основании следующих определяющих признаков:

– для «ИСПДн КБ» характерны угрозы 3-го типа;

– «ИСПДн КБ» обрабатывает иные категории персональных данных сотрудников оператора.

Вывод: 4 уровень защищённости персональных данных при их обработке в «ИСПДн КБ» определён в соответствии с действующей нормативной документацией.

4.5 Проверка уровня подготовки кадров и распределения ответственности за выполнение требований по защите информации на объекте вычислительной техники

Список пользователей «ИСПДн КБ» и приказ о назначении АИБ Утвержен. Утверждено описание технологического процесса обработки информации в «ИСПДн КБ».

Вывод: проведено интервьюирование АИБ, проверены уровень профессиональной подготовки кадров и распределение ответственности за выполнение требований по защите информации между участниками процесса обработки конфиденциальной информации.

4.6 Проверка наличия сертификатов соответствия средств защиты информации

Перечень программных средств защиты информации (СЗИ) приведен в таблице 3.

Продолжение приложения К

Таблица 3 – Перечень программных СЗИ

№	Наименование	Сертификат
1.	Операционная система Microsoft Windows 7 Профессиональная	Сертификат ФСТЭК № 2180/1 от 04.10.2011 (Действителен до 04.10.2020)
2.	Межсетевой экран Cisco ASA 5540	Сертификат ФСТЭК № 3677 от 30.11.2016 (Действителен до 30.11.2019)
3.	Программа антивирусной защиты Kaspersky Endpoint Security 10	Сертификат ФСТЭК № 3025 от 25.11.2013 (Действителен до 25.11.2019)

Вывод: перечень представленных сертификатов достаточен и их содержание соответствует требованиям по безопасности программных средств защиты информации для информационной системы с 4 уровнем защищённости персональных данных.

4.7 Проверка достаточности принятых организационных мер по ограничению доступа посторонних лиц к техническим средствам обработки защищаемой информации, носителям информации и каналам передачи информации

Используемые средства защиты информации позволяют выполнить требования руководящих документов по безопасности информации, обрабатываемой в «ИСПДн КБ».

Вывод: принятые организационные меры по ограничению доступа посторонних лиц к техническим средствам обработки защищаемой информации, носителям информации и каналам передачи информации являются достаточными для обеспечения необходимого уровня защищенности.

4.8 Выводы и рекомендации

Комиссия отмечает, что:

– перечень представленных нормативных и организационно-распорядительных документов является достаточным;

– классификация «ИСПДн КБ» проведена, уровень защищённости персональных данных при их обработке в «ИСПДн КБ» установлен обоснованно и в соответствии с требованиями действующей нормативной документации;

Продолжение приложения К

– состав и структура программно-технических средств «ИСПДн КБ» соответствует представленной документации;

– помещение, в котором устанавливаются СВТ для обработки информации с ограниченным доступом, соответствует требованиям по безопасности информации;

– все представленные комиссии сертификаты соответствия требованиям по безопасности информации являются действующими на момент проведения аттестационных испытаний;

– принятые организационные меры по ограничению доступа посторонних лиц к техническим средствам обработки защищаемой информации, носителям информации и каналам передачи информации являются достаточными для обеспечения необходимого уровня защищенности «ИСПДн КБ».

Исходя из вышеизложенного, комиссия делает вывод о том, что объект информатизации «Информационная система персональных данных клиент-банка» соответствует организационным требованиям по защите информации по 4 уровню защищённости.

Председатель комиссии М.А. Арасланов

Члены комиссии: М.О. Бушуев

Д.С. Силантьев

Окончание приложения К

ПРИЛОЖЕНИЕ Л

ГОСУДАРСТВЕННОЕ ПРЕДПРИЯТИЕ

УТВЕРЖДАЮ

Заместитель генерального
директора по безопасности

_____ С.В. Перфилов

____ . _____ . 2018

ПРОТОКОЛ

аттестационных испытаний объекта информатизации
«Информационной системы персональных данных клиент-банка»
на соответствие требованиям по защите информации от несанкционированного доступа

№ 435/90

Начальник службы безопасности

_____ В.А. Кашуба

____ . _____ . 2018

2018

Продолжение приложения Л

1.Общие сведения об объекте

1.1 Аттестационная комиссия в составе: М.А. Арасланов, М.О. Бушуев, Д.С. Силантьев провела аттестационные испытания объекта информатизации на соответствие требованиям по защите информации от несанкционированного доступа.

1.2 Заявитель аттестационных испытаний объекта – управление информационных технологий государственного предприятия.

1.3 Наименование объекта: «Информационная система персональных данных клиент-банка» («ИСПДн КБ»).

1.4 Расположение объекта: г. Озерск, ул. Герцена 7, пом. 226.

2. Состав и классификация объекта

2.1 Уровень защищенности персональных данных при их обработке в информационной системе - четвертый. Объект информатизации не подлежит категорированию, так как в данной системе не обрабатываются сведения, составляющие государственную тайну

2.2 Для аттестационных испытаний был представлен объект информатизации на базе персональной электронно-вычислительной машины, имеющей подключение к сети общего доступа Интернет.

Комплектация объекта информатизации указана в таблице 1.

Состав программного обеспечения и средств защиты информации, используемых в ИС, приведены в таблице 2 и таблице 3 соответственно.

Продолжение приложения Л

Таблица 1 – Комплектация объекта информатизации

№	Наименование устройства	Модель	Заводской номер
1.	Системный блок	IRU Brava Home 114W	10157
2.	Монитор	Samsung S27A750D	ETL460C260723157E
3.	Клавиатура	Genius KM-122	ZM6C02019509
4.	Мышь	A4Tech X7 XL-750BX	130-130009-200
5.	МФУ	Samsung SCX-4100	CNKDS08892

Таблица 2 – Состав программного обеспечения

№	Наименование программных средств	Сведения о лицензии
1.	Microsoft Windows 7 Профессиональная	Корпоративная лицензия
2.	Microsoft Office Professional 2010	Корпоративная лицензия
3.	«Клиент-банк»	Корпоративная лицензия
4.	Программа антивирусной защиты Kaspersky Endpoint Security	Корпоративная лицензия
5.	Интернет браузер Opera	свободно распространяемое

Таблица 3 – Перечень средств защиты информации

№	Наименование	Сертификат
1.	Операционная система Microsoft Windows 7 Профессиональная	Сертификат ФСТЭК № 2180/1 от 04.10.2011 (Действителен до 04.10.2020)
2.	Межсетевой экран Cisco ASA 5540	Сертификат ФСТЭК № 3677 от 30.11.2016 (Действителен до 30.11.2019)
3.	Программа антивирусной защиты Kaspersky Endpoint Security 10	Сертификат ФСТЭК № 3025 от 25.11.2013 (Действителен до 25.11.2019)

3. Объем проводимых аттестационных испытаний объекта информатизации на соответствие требованиям по защите информации от несанкционированного доступа

3.1 Испытания проводились в объеме, предусмотренном «Программой и методиками проведения аттестационных испытаний объекта информатизации – «Информационной системы клиент-банка» на соответствие требованиям по безопасности информации» и включали в свой состав:

Продолжение приложения Л

– проверка наличия сертификатов на средства защиты информации, выполнения правил их эксплуатации;

– проверка соответствия описания технологического процесса обработки и хранения защищаемой информации реальному процессу;

– испытания подсистемы управления доступом;

– испытания подсистемы регистрации событий безопасности;

– испытание подсистемы антивирусной защиты;

– проверка установки обновлений программного обеспечения и средств защиты информации;

– проверка подсистемы межсетевого экранирования;

– проверка обеспечения физической охраны СВТ.

3.2 При проведении аттестационных испытаний применялись следующие методы проверок и испытаний:

– экспертно-документальный метод;

– проверка функций или комплекса функций защиты информации от несанкционированного доступа с помощью инструментальных средств контроля, а также путем пробного запуска СЗИ от НСД и наблюдения за выполнением их функций;

– попытка «взлома» системы защиты информации;

– проверка соответствия примененных параметров настройки элементов системы защиты информации требованиям безопасности информации;

– проверка подсистем защиты информации от НСД, целостности применяемых СЗИ от НСД, в том числе с использованием специальных средств контроля эффективности защиты информации;

– проверка программной совместимости и корректности функционирования всего комплекса используемых СВТ с продукцией, используемой в целях защиты информации;

– испытания системы защиты информации от НСД путем попыток

Продолжение приложения Л

осуществить НСД к тестовой защищаемой информации в обход используемой системы защиты информации.

4.Протокол проверки соответствия СЗИ

4.1 Проверка наличия сертификатов на средства защиты информации, выполнения правил их эксплуатации

При проверке образцов СЗИ от НСД использовалась документация разработчика по СЗИ от НСД (носители с дистрибутивами, сопроводительная документация, знаки соответствия, копии сертификатов соответствия, формуляры, технические условия, руководства для администратора информационной безопасности).

Настройка защитных механизмов ОС выполнена в соответствии с руководством «Операционная система Microsoft Windows 7. Руководство по настройке функций безопасности сертифицированной версии».

Вывод: Применяемые средства защиты соответствуют требованиям нормативных документов для обеспечения безопасности персональных данных при обработке в ИС с 4 уровнем защищенности.

Используемые СЗИ имеют действующие сертификаты соответствия ФСТЭК России.

Установка СЗИ выполнена с дистрибутивов, приобретённых у официальных поставщиков, имеющих специальные защитные знаки и формуляры.

4.2 Проверка соответствия описания технологического процесса обработки и хранения защищаемой информации реальному процессу

Для проверки соответствия описания технологического процесса обработки защищаемой информации реальному процессу комиссии были представлены документы, указанные в таблице 4.

Продолжение приложения Л

Таблица 4 – Перечень документации на объект информатизации

№	Наименование документа	Номер документа
14.	Техническое задание на создание системы защиты информации в ИС	ЕЕ.338758.В20 1В
15.	Описание технологического процесса обработки информации	ЕЕ.338754.В20 РА
16.	Технический паспорт ИС	ЕЕ.14082.К58 КЭ
17.	Акт классификации ИС	4.2.1./1915
18.	Инструкция типовая, технологическая по обеспечению защиты конфиденциальной информации	И-046-2018
19.	Инструкция типовая, технологическая администратора ИБ и АС	И-037-2018
20.	Инструкция типовая, технологическая для технического обслуживающего персонала	И-029-2018
21.	Приказ о создании комиссии для проведения аттестационных испытаний объекта информатизации	НН.3872 АК
22.	Приказ о назначении пользователей, ответственных за обеспечение безопасности персональных данных	НН.2836 ЧС
23.	Акты обследований помещений на соответствие требованиям по защите персональных данных	543.43/548
24.	Заключение экспертной комиссии	47/4
25.	Перечень защищаемых ресурсов	324.43/1

№	Наименование документа	Номер документа
26.	Список пользователей, допущенных до работы в ИС	4398.5 РО

Объектами доступа являются:

– программные средства ОИ, предназначенные для обработки информации;

– учтенные машинные носители информации – НЖМД и флэш накопители.

Субъектами доступа в ИС являются пользователи, администраторы и процессы, выполняемые от их имени, которые имеют возможность доступа к объектам штатными средствами. Субъектам доступа присваиваются права и полномочия на уровне системы разграничения доступа операционной системы и межсетевого экрана.

Продолжение приложения Л

В процессе анализа технологического процесса обработки информации в ИС установлено, что все субъекты доступа идентифицируются по имени учетной записи и аутентифицируются по паролям штатными средствами домена безопасности «Inet-Mayak.ru».

Вывод: Описание технологического процесса обработки и хранения защищаемой информации соответствует реальному процессу.

4.3 Подсистема управления доступом

Проверка наличия и работоспособности подсистемы идентификации

Проверялась правильность идентификации субъектов доступа путем обращения субъектов доступа ИС к объектам доступа при помощи штатных средств. При обращении проводилась проверка принадлежности предъявленного субъектом идентификатора множеству всех зарегистрированных в системе идентификаторов. При предъявлении идентификатора, не известного подсистеме идентификации, средства управления прекращали процесс предоставления доступа.

Вывод: проверка выполнена успешно.

Проверка наличия и надежности подсистемы аутентификации

Проверялась правильность аутентификации субъектов доступа. При предъявлении пароля, соответствующего идентификатору субъекта, средства управления предоставляли доступ в операционную систему. При предъявлении пароля, не соответствующего идентификатору субъекта, средства управления блокировали доступ в операционную систему.

Проверялась возможность компрометации пароля методом его подбора. Были выполнены попытки ввода неверного пароля, а также проанализированы применяемые политики безопасности.

Вывод: проверка выполнена успешно.

Проверка отсутствия условий компрометации подсистемы идентификации и аутентификации

Проверялась возможность несанкционированного изменения информации об идентификации и аутентификации. Доступ субъектов ИС к файлам, содержащим информацию об идентификации и аутентификации, полностью закрыт для прикладных программ. На СВТ, входящих в состав ИС, отсутствуют прикладные программные средства прямого доступа к устройствам и оперативной памяти, средства разработки и отладки программ.

Вывод: проверка выполнена успешно.

Проверка времени действия пароля

В ИС был произведен перевод системного времени на год вперед и осуществлен вход пользователя в систему. Подсистема идентификации и аутентификации разрешила вход пользователя в систему и вывела сообщение с предложение смены пароля.

Вывод: проверка выполнена успешно.

Проверка длины пароля

В локальной политике безопасности минимальная длина пароля установлена в 6 символов. Для запуска данной оснастки необходимы привилегии администратора операционной системы. Попытка установки пользователем пароля короче 6 символов завершилась безуспешно.

Вывод: проверка выполнена успешно.

4.4 Подсистема регистрации событий безопасности

4.4.1 Проверка регистрации начала и окончания работ

Проверка осуществлялась штатными средствами ИС. Проводилась загрузка операционной системы и запуск программных комплексов ИС, предусмотренных технологией инициализации ИС. Осуществлялись попытки входа в систему по неверному идентификатору доступа, по верному идентификатору доступа и неверному паролю, по идентификатору и паролю легитимного субъекта доступа. Производился программный останов ИС. Производился вход в систему с правами

администратора ИБ и исследование журнала регистрации доступа. При этом регистрационные записи для каждого события содержали:

– дату и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;

– результат попытки входа: успешная или неуспешная — несанкционированная.

Вывод: проверка выполнена успешно.

4.4.2 Проверка регистрации выдачи документов на «твердую» копию

Была произведена печать тестовой страницы, затем проведена проверка журнала PrintServise.

Вывод: проверка выполнена успешно.

4.5 Проверка подсистемы антивирусной защиты

В ИС используется антивирусное ПО Kaspersky Endpoint Security 10. Антивирусные базы периодически обновляются. Установлен пароль администратора для данного ПО.

Вывод: проверка выполнена успешно.

4.6 Проверка установки обновлений ПО и СЗИ

Произведена установка необходимых сертифицированных обновлений безопасности ОС и СЗИ.

Вывод: Установка выполнена успешно.

4.7 Проверка подсистемы межсетевого экранирования

В качестве межсетевого экрана используется Cisco ASA 5540 с действующим сертификатом соответствия ФСТЭК России. Межсетевой экран настроен в соответствии с документацией

Вывод: проверка выполнена успешно.

Продолжение приложения Л

4.8 Проверка обеспечения физической охраны СВТ (устройств и носителей информации)

Имеется акт обследования помещения на соответствие требованиям безопасности персональных данных, подтверждающих наличие средств контроля доступа в помещение посторонних лиц, особенно в нерабочее время.

Вывод: проверка выполнена, техническая оснащенность помещения удовлетворяет требованиям безопасности персональных данных.

Результаты проведенных проверок показали, что объект информатизации «Информационная система персональных данных клиент-банка», обрабатывающий персональные данные, по совокупности используемых настроек политики безопасности, используемых средств защиты информации и принятых

организационных мер соответствует требованиям, предъявляемых к информационным системам с 4 уровнем защищенности персональных данных.

Председатель комиссии	М.А. Арасланов
Члены комиссии:	М.О. Бушуев
	Д.С. Силантьев

Окончание приложения Л

ПРИЛОЖЕНИЕ М

ГОСУДАРСТВЕННОЕ ПРЕДПРИЯТИЕ

УТВЕРЖДАЮ

Заместитель генерального
директора по безопасности

_____ С.В. Перфилов

____ . _____ . 2018

Информационная система персональных данных клиент-банка
ЗАКЛЮЧЕНИЕ

По результатам аттестационных испытаний

Начальник службы безопасности	Начальник управления информационных технологий
_____ В.А. Кашуба	_____ В.Е. Кочетков
____ . _____ . 2018	___ . _____ . 2018

2018

Продолжение приложения М

Аттестационная комиссия в составе: М.А. Арасланов, М.О. Бушуев, Д.С. Силантьев провела аттестационные испытания в соответствии с «Программой и методикой проведения аттестационных испытаний информационной системы персональных данных клиент-банка» (№ 30/95 ДС).

Результаты аттестационных испытаний приведены в протоколах по направлениям:

– проверка объекта на соответствие организационно-техническим требованиям (№ 789/12);

– защита от несанкционированного доступа (№ 435/90);

Заявитель аттестационных испытаний объекта – УИТ государственного предприятия.

Комиссия считает, что реализованные средства и меры защиты информации на объекте информатизации «Информационной системе персональных данных клиент-банка», размещенном по адресу: г. Озерск, ул. Герцена, д. 7, 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	М.А. Арасланов
Члены комиссии:	М.О. Бушуев
	Д.С. Силантьев

Окончание приложения М

ПРИЛОЖЕНИЕ Н

ГОСУДАРСТВЕННОЕ ПРЕДПРИЯТИЕ

УТВЕРЖДАЮ

Заместитель генерального
директора по безопасности

_____ С.В. Перфилов

____ . _____ . 2018

Информационная система персональных данных клиент-банка

Аттестат соответствия

Выдан: 21 мая 2018 г.

Действителен до: 21 мая 2021 г.

Начальник службы безопасности

_____ В.А. Кашуба

____ . _____ . 2018

2018

Продолжение приложения Н

Настоящим Аттестатом удостоверяется, что объект информатизации (ОИ) «Информационная система персональных данных клиент-банка» УИТ государственного предприятия (далее ИСПДн КБ) уровня защищенности «4», размещенная по адресу: г. Озерск, ул. Герцена, д. 7, 2 этаж, кабинет № 226 соответствует требованиям нормативной документации по безопасности персональных данных.

Состав комплекса технических средств ИСПДн КБ, схема размещения в помещении и относительно границ контролируемой зоны, перечень используемых программных средств, а также средств защиты приведены в техническом паспорте на объект информатизации (ЕЕ.14082.К58 КЭ).

Организационная структура, уровень подготовки специалистов, нормативно-методическое обеспечение и техническая оснащённость организации обеспечивают контроль эффективности мер и средств защиты и поддержание уровня защищённости ИСПДн КБ в процессе эксплуатации в соответствии с установленными требованиями.

Аттестация ИСПДн КБ выполнена в соответствии с программой и методикой аттестационных испытаний, утвержденными руководителем органа по аттестации № 346 от 19.05.2018 г.

С учетом результатов аттестационных испытаний ИСПДн КБ разрешается обработка персональных данных категории «Иные».

Контроль за эффективностью реализованных мер и средств защиты возлагается на ответственного за обеспечение безопасности персональных данных.

Подробные результаты аттестационных испытаний приведены в заключении по результатам аттестационных испытаний № 357 от 21.05.2018 г. и протоколах испытаний.

«Аттестат соответствия» выдан на три года, в течение которых должна быть обеспечена неизменность условий функционирования ИСПДн КБ и технологии обработки защищаемой информации, способных повлиять на характеристики, указанные ниже.

Продолжение приложения Н

При окончании срока действия сертификата соответствия ФСТЭК России на средство защиты информации, должна проводиться процедура продления срока действия сертификата соответствия. Эта процедура осуществляется производителем средства защиты информации. Если производитель не осуществляет продление срока действия сертификата соответствия, продление должно осуществляться организацией, эксплуатирующей средство защиты информации, в индивидуальном порядке. Порядок продления срока действия сертификатов соответствия организациями, эксплуатирующими средства защиты

информации, определен в документе ФСТЭК России «Информационное сообщение по вопросу продления
сроков действия сертификатов соответствия на средства защиты информации, эксплуатируемые на объектах информатизации»

Перечень характеристик, об изменении которых требуется обязательно извещать орган по аттестации:

– состав оборудования ОИ;

– условия размещения ОИ и его технических средств;

– характеристики систем (защиты информации, электропитания, заземления, сигнализации) обеспечения эксплуатации ОИ.

При эксплуатации ИСПДн КБ запрещается:

– вносить изменения в комплектность ИСПДн, 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;

– 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.

Председатель комиссии М.А. Арасланов

Окончание приложения Н