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, директор ООО «Центр защиты информации «Эгида»
_____И.У. Кулдыбаева
_____ 2018 г.

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

Модернизация защиты информационной системы персональных данных в Таможенном управлении

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ – 10.05.03.2018.263.ПЗ ВКР

Консультанты

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

Руководитель проекта, доцент
_____ В.Ю. Бердюгин
_____ 2018 г.

Автор проекта, студент группы КЭ-530
_____А.Н. Дьяконов
_____ 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

Дьяконова Александра Николаевича

Группа ____*КЭ-530*

1. Тема работы

Модернизация защиты информационной системы персональных данных в Таможенном управлении

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

1. Срок сдачи студентом законченной работы _____*27.05.2018*_____

2. 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)

4.1 Анализ ИСПДН на соответствие требованиям по защите информации для информационных систем, регламентируемых действующим законодательством РФ в области информационной безопасности

4.2 Теоретическое обоснование реализации средств и методов защиты информации

4.3 Модернизация системы защиты ИСПДн «ОПСУР»

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

Презентация к выпускной квалификационной работе на тему: «Модернизация защиты информационной системы персональных данных в Таможенном управлении»

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 *25 января 2018*

Руководитель,
доцент _____ В.Ю. Бердюгин

Задание принял к исполнению _____ А.Н. Дьяконов

КАЛЕНДАРНЫЙ ПЛАН

Наименование этапов выпускной квалификационной работы (проекта)	**Срок выполнения этапов работы**	**Отметки о выполнении руководителя**
Введение		
1 Анализ ИСПДН на соответствие требованиям по защите информации для информационных систем, регламентируемых действующим законодательством РФ в области информационной безопасности		
2 Теоретическое обоснование реализации средств и методов защиты информации		
3 Модернизация системы защиты ИСПДн «ОПСУР»		
4 Безопасность жизнедеятельности		
Заключение		
Библиографический список		
Предзащита ВКР		
Защита ВКР		

Заведующий кафедрой _____ А.Н. Соколов

Руководитель работы _____ В.Ю. Бердюгин

Студент _____ А. Н. Дьяконов

АННОТАЦИЯ

Дьяконов А.Н. Модернизация защиты информационной системы персональных в Таможенном управлении – Челябинск: ЮУрГУ, КЭ-530, 190 с., 1 ил., 9 табл., библиогр. список – 15 наим., 6 прил.

Выпускная квалификационная работа выполнена с целью модернизации защиты информационной системы персональных данных в Таможенном управлении. Работа состоит из трех глав.

В первой главе проведен анализ информационной системы персональных данных на соответствие требованиям по защите информации для информационных систем, регламентируемых действующим законодательством РФ в области информационной безопасности

Во второй главе выявлены актуальные угрозы, рассмотрены пути их нейтрализации, представлено теоретическое обоснование реализации средств и методов защиты информации.

В третей главе разработан проект по модернизации защиты информационной системы персональных данных «ОПСУР».

ОГЛАВЛЕНИЕ

СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ

АРМ – автоматизированное рабочее место;
БД – база данных;
ВП – вредоносная программа;
ИС – информационная система;
ЛВС – локальная вычислительная сеть;
НЖМД – накопитель на жестких магнитных дисках;
НСД – несанкционированный доступ;
ОС – операционная система;
ОТСС – основные технические средства и системы;
ПАК – программно-аппаратный комплекс;
ПДн – персональные данные;
ПК – программный комплекс;
ПО – программное обеспечение;
ПЭВМ – персональная электронно-вычислительная машина;
СЗИ – средство защиты информации;
СЗИ от НСД – средство защиты информации от несанкционированного доступа;
СКЗИ – средство криптографической защиты информации;
СПЗ – служебное производственное здание;
ТЗ – техническое задание;
ТП – технологический процесс;
ОПСУР – отдел применения системы управления рисками;
ЕБВР – единая база выявления рисков.

Автоматизированное рабочее место (АРМ) – программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида.

Администрирование – этап технологического процесса, на котором производятся служебные операции как с хранимой информацией (резервирование и восстановление), так и с программными средствами обработки и защиты информации.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

Ввод информации – этап технологического процесса, на котором производится создание либо перемещение информации с внешних носителей на внутренние носители (несъемные МН).

Вывод информации – этап технологического процесса, на котором производится перемещение информации с внутренних МН на внешние носители (в том числе монитор).

Дискреционное управление доступом – разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих их обработку информационных технологий и технических средств.

Машинные носители информации (МН) – магнитные, оптические и прочие хранилища информации, используемые в средствах вычислительной техники, в т.ч. съемные (НГМД, CD, DVD, Flash-накопители, магнитные ленты и др.) и несъемные (НЖМД, HDD).

Несанкционированный доступ к информации (НСД) – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами. Примечание. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем.

Обработка информации – этап технологического процесса, на котором производится преобразование информации, полученной на этапе ввода или хранимой в структурированном виде, для последующего ее вывода или хранения.

Объект доступа – единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

Система защиты информации от несанкционированного доступа (СрЗИ НСД) – комплекс организационных мер и программно- технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации в автоматизированных системах.

Средство защиты от несанкционированного доступа (Средство защиты от НСД) – программное, техническое или программно- техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа.

Средство криптографической защиты информации (СКЗИ) – средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности.

Субъект доступа – Лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технологический процесс обработки информации (ТП) – последовательность действий пользователей при работе с информацией, включающая следующие этапы: ввод, обработку (преобразование), хранение, передачу, вывод, администрирование (резервирование, управление доступом).

Техническое обслуживание – этап технологического процесса, на котором производятся служебные операции с аппаратными средствами обработки и защиты информации.

Хранение информации – этап технологического процесса, на котором информация размещается в структурированном виде в период между двумя любыми этапами технологического процесса.

ВВЕДЕНИЕ

Развитие информационных технологий довольно сильно изменило многие аспекты трудовой деятельности. Если еще 30 лет назад компьютеры использовались исключительно для сложнейших расчетов и управления техническими процессами, то сейчас повсеместная информатизация привела к использованию компьютеров для автоматизации однотипных, а порой рутинных процессов, к каким, в том числе, можно и отнести обработку и передачу персональных данных, служебной информации. Однако подобный подход определил новый ряд проблем. Информация теперь не занимает большого пространства, легко и неконтролируемо модифицируется и копируется. Удобная, структурированная, она стала объектом внимания злоумышленников, которым, порой, не требовалось и личного присутствия для ее перехвата или изменения. Организация защиты информации легла на ее владельцев, а в случае федеральных органов – на государство. Острее стоит проблема в областях, взаимодействующих с иностранными государствами. В таких случаях злоумышленником может выступать международный преступный синдикат, который, зачастую, более подготовлен и оснащен, нежели локальный вредитель. И потому к таким объектам применяются повышенные меры защиты.

Объектом выпускной квалификационной работы является Таможенное управление.

Предметом дипломной работы является система защиты информационной системы персональных данных Таможенного управления.

Целью выпускной квалификационной работы является модернизация защиты информационной системы персональных данных в Таможенном управлении.

Для достижения поставленной цели необходимо произвести:

1. анализ ИСПДн на соответствие требованиям по защите информации для информационных систем, регламентируемых действующим законодательством РФ в области информационной безопасности, а именно:

– анализ организационной структуры объекта информатизации, информационных потоков, разработанной документации и ее соответствия требованиям нормативной документации по защите информации;

– анализ текущих средств защиты информации;

– определение структуры системы защиты информации и ее подсистем;

– анализ состава и структуры комплекса технических средств и программного обеспечения, системы защиты информации на объекте.

2. теоретическое обоснование реализации средств и методов защиты информации, а именно:

– анализ угроз;

– нейтрализация угроз;

– программно-аппаратные средства;

– организационные меры.

3. модернизация системы защиты ИСПДн «ОПСУР», а именно представить:

– стадии реализации;

– основные технические решения;

– архитектурные решения СЗИ;

– применяемые средства защиты информации;

– подсистему организационно-правовых мероприятий;

– идентификацию и аутентификацию субъектов доступа и объектов доступа;

– управление доступом субъектов доступа к объектам доступа;

– ограничение программной среды;

– защиту машинных носителей информации;

– регистрацию событий безопасности;

– антивирусную защиту;

– контроль (анализ) защищенности информации;

– обеспечение целостности информационной системы и информации;

– обеспечение доступности информации;

– защиту технических средств;

– мероприятия по подготовке к вводу СЗИ в действие;

– организационно-технические меры защиты информации от несанкционированного доступа.

1.АНАЛИЗ ИСПДН НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ПО ЗАЩИТЕ ИНФОРМАЦИИ ДЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ, РЕГЛАМЕНТИРУЕМЫХ ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ РФ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Общие сведения

Анализ системы начинается с ее обследования. Для получения наиболее объективной и полной информации о защищаемом объекте необходимо выполнить следующие действия:

1. получить общие сведения об объекте защиты, Учреждении и его деятельности;
2. произвести осмотр зданий и помещений Учреждения, в которых ведется обработка информации;
3. выделить из общего набора информацию ограниченного распространения;
4. исследовать технологический процесс обработки, хранения и передачи информации;
5. провести интервьюирование сотрудников Учреждения, выполняющих обработку защищаемой информации;
6. проанализировать имеющиеся в Учреждении документы, связанные с обработкой информации ограниченного распространения;
7. выполнить контрольно-измерительные мероприятия.

Обследование ИС проводится с целью определения исходных данных системы для разработки частной модели угроз безопасности персональных данных, обрабатываемых в ИС и создания системы защиты персональных данных ИС в соответствии с требованиями нормативных документов Российской Федерации.

Обследование и анализ ИС Таможенного управления проведены в соответствии со следующими нормативными правовыми актами:

– Приказ Федеральной таможенной службы России от 11.08.2015 г. № 1611 «Об утверждении требований по обеспечению безопасности персональных данных в таможенных органах Российской Федерации, организациях, находящихся в ведении ФТС России, при их обработке в информационных системах персональных данных таможенных органов Российской Федерации».

– Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

– Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

– Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

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

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

– Специальные требования и рекомендации по технической защите конфиденциальной информации (утв. приказом № 282 Гостехкомиссии России от 30 августа 2002 г.).

– 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».

– Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная ФСТЭК России 15 февраля 2008 г.

– Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная ФСТЭК России 14 февраля 2008 г.

– Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утвержденные ФСБ РФ 21 февраля 2008 г. № 149/54-144.

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

– Приказ ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

– Приказ ФСБ РФ от 9 февраля 2005 г. № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (положение ПКЗ-2005)».

Обследование ИС Таможенного управления было проведено методами:

– опроса (анкетирования) специалистов, эксплуатирующих ИС;

– изучения документации по вопросам защиты информации в ИС;

– непосредственного посещения ИС.

В ходе проведения работ по обследованию ИС Таможенного управления была предоставлена следующая информация:

– данные об информационных ресурсах, подлежащих защите;

– информация о технологии обработки информации в ИС;

– существующий порядок доступа к информационным ресурсам ИС;

– информация о составе, размещении и характеристиках комплекса используемых технических средств (серверов, автоматизированных рабочих мест и сетевого оборудования);

– информация о решаемых задачах и настройках программно-технических средств;

– другая необходимая информация.

В соответствии с целями обследования ИС Таможенного управления были выполнены следующие основные работы:

– описание текущего состояния защищенности ИС;

– инвентаризация информационных ресурсов ИС, подлежащих защите;

– инвентаризация аппаратного и программного обеспечения ИС;

– анализ технологии обработки информации в ИС;

– определение конфигурации и топологии ИС и систем связи как внутри информационной системы, так и во взаимодействии с другими системами различного уровня и назначения;

– анализ выполнения требований нормативных правовых актов по вопросам защиты информации и персональных данных;

– обследование структурированной кабельной системы ИС на предмет ее пригодности для обеспечения защиты информации;

– разработка проектов организационно-распорядительных документов Таможенного управления и других документов.

1.2. Описание объекта информатизации

Объект информатизации ИСПДн «ОПСУР» состоит из шести автоматизированных рабочих мест, расположенных следующим образом:

– 4 АРМ в различных служебных производственных зданиях таможенных постов, расположенных на непосредственной границе РФ;

– 2 АРМ на 3 этаже административного здания Таможенного управления.

Структурное подразделение, эксплуатирующее ИС: отдел применения системы управления рисками Таможенного управления.

АРМ в составе ИС соединены в локальную сеть Таможенного управления на основе защищенного канала связи, реализованного на базе сети международного информационного обмена (Интернет).

ИС имеет подключение к АИС «ЕБВР», расположенную на сервере центрального аппарата в г. Москва и содержащую базу данных.

Передача данных осуществляется по защищенному каналу связи с помощью средств криптографической защиты информации «Континент».

Основным назначением ИС является автоматизация обмена информации о проведении таможенного контроля подчиненными таможенными органами, а также сбор, обобщение и анализ отчетности подчиненных таможенных органов.

По режиму обработки информации ИС относится к многопользовательским системам. Пользователями ИС являются сотрудники отдела применения системы управления рисками, которым в соответствии с занимаемой должностью предоставлены различные права доступа к информации, обрабатываемой в ИС.

1.3. Процессы обработки конфиденциальной информации (персональных данных)

В ИС осуществляется обработка персональных данных (далее – ПДн). ИС является информационной системой, обрабатывающей ПДн иных категорий субъектов персональных данных, являющихся сотрудниками Таможенного управления и не являющихся сотрудниками Таможенного управления.

Обработка ПДн в ИС осуществляется в целях обеспечения соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации, обеспечения кадровой работы, содействия сотрудникам Таможенного управления в прохождении государственной гражданской службы Российской Федерации, анализа и контроля совершения таможенных операций в отношении перемещаемых через таможенную границу РФ товаров и транспортных средств международной перевозки, в том числе в целях выявления и предотвращения случаев нарушения требований таможенного законодательства.

В ИС обрабатываются персональные данные менее чем 100 000 субъектов ПДн. В ИС осуществляется обработка следующих категорий субъектов ПДн:

– государственные гражданские служащие – сотрудники Таможенного управления;

– лица, замещающие государственные должности Таможенного управления и их заместители;

– граждане Российской Федерации, обратившиеся в Таможенное управление с целью перемещения через таможенную границу РФ товаров и транспортных средств международной перевозки;

– иностранные граждане, обратившиеся в Таможенное управление с целью перемещения через таможенную границу РФ товаров и транспортных средств международной перевозки.

Взаимодействие ИС с внешними информационными системами не осуществляется.

Уполномоченные сотрудники отдела применения системы управления рисками Таможенного управления получают сведения о персональных данных субъектов ПДн из следующих документов:

– паспорт или иной документ, удостоверяющий личность;

– документы, подтверждающие усыновление, опекунство или попечительство несовершеннолетнего лица;

– документы, подтверждающие стоимость декларируемых товаров для личного пользования;

– транспортные (перевозочные) документы;

– документы, подтверждающие право на льготы по уплате таможенных платежей, в том числе подтверждающие временный ввоз (вывоз) физическим лицом товаров для личного пользования, а также подтверждающие признание физического лица беженцем, вынужденным переселенцем, либо переселяющимся на постоянное место жительства;

– документы, подтверждающие соблюдение ограничений, кроме мер нетарифного и технического регулирования;

– документы, содержащие сведения, позволяющие идентифицировать транспортное средство для личного пользования;

– документы, подтверждающие право владения, пользования и (или) распоряжения транспортным средством личного пользования;

– иные документы и сведения, представление которых предусмотрено в соответствии с таможенным законодательством Таможенного союза.

Полученные ПДн подлежат дальнейшей автоматизированной обработке в ИС.

Работа пользователей ИС определяется утвержденной инструкцией пользователя. Данные поступают на бумажных носителях. Сотрудник вручную вносит данные в БДн АИС «ЕБВР» путем заполнения формы в веб-приложении.

Данные хранятся на сервере баз данных в центральном аппарате г. Москва. Передача осуществляется по защищенному каналу связи. Права доступа пользователей к режимам обработки файлов (ввод, корректировка, просмотр, печать) утверждаются в установленном порядке. Работа пользователя возможна только после успешного прохождения процедуры аутентификации в веб-приложении АИС «ЕБВР».

Перечень ПДн, обрабатываемых в ИС Таможенного управления, приведен в таблице 1.

Таблица 1 – Перечень ПДн

№ п/п	Способ обработки ПДн	Перечень ПДн
1	2	3
1	Автоматизированная обработка в ИС	фамилия, имя, отчество (при наличии); данные об отправителе - краткое наименование организации и место ее нахождения или обособленного подразделения организации; данные документа, удостоверяющего личность (вид, серия, номер, дата выдачи, наименование органа, выдавшего документ) адрес и дата регистрации по месту жительства;

Продолжение таблицы 1

1	2	3
		адрес фактического проживания; банковские реквизиты: номер счета, наименование и адрес банка, номер корреспондентского счета, срок оплаты и другие данные, необходимые для осуществления платежа; номера и даты коммерческих документов, имеющихся у декларанта (счет на оплату и поставку товаров, счет-фактура (инвойс), счет-проформа (проформа-инвойс) и др.); номер и дата выдачи сертификата о происхождении товаров, код страны в соответствии с Классификатором стран мира; информация о транспортной накладной – дата документа, наименование и адрес отправителя и перевозчика, места, даты принятия груза и места, предназначенного для его доставки, наименование и адрес получателя и т.д.; принятое обозначение характера груза и род его упаковки; платежи, связанные с перевозкой (таможенные пошлины и сборы и т.д.), и другие платежи, взимаемые с момента заключения договора до сдачи груза.

1.3. Сведения об организации безопасности информации на ОИ

1.3.1. Технические средства охраны и физическая безопасность на ОИ

Учреждение расположено в административных зданиях.

Все технические средства ИС расположены в пределах границы контролируемой зоны, которой являются стены помещений.

Охрана помещений, занимаемых объектом осуществляется охранным предприятием. Вход в здания оборудован круглосуточным постом охраны.

Обследуемые помещения оборудованы исправными системами охранной и пожарной сигнализации и системой кондиционирования.

Коридоры (подступы к обследуемым помещениям) оборудованы видеокамерами круглосуточного наблюдения, а в случае таможенных постов на границе – охраняемым периметром.

Система электропитания зданий резерва не имеет.

Для защиты от утечек информации по видовым каналам оконные проемы помещений оснащены жалюзи.

1.3.2. Оборудование, обслуживание помещений, расположение элементов ОИ, средства и методы защиты информации

Здания, в которых располагаются элементы обследуемого ОИ:

– СПЗ №1-СПЗ №4: двухэтажное, капитальное кирпичное.

– здание таможенного управления: четырехэтажное, капитальное кирпичное.

Двери помещений - типовые стальные, все двери оборудованы исправными замками с комплектами ключей к ним.

Обслуживание всех систем жизнеобеспечения обследуемых помещений осуществляется ответственными лицами Таможенного управления с привлечением сторонних обслуживающих предприятий, организаций на контрактной основе.

Обслуживание систем жизнеобеспечения помещений осуществляется только в присутствии работников, выполняющих в них свои должностные обязанности в связи с эксплуатацией ИСПДн «ОПСУР». Уборка помещений осуществляется во внерабочем времени в отсутствие вышеозначенных работников.

Мониторы ПЭВМ установлены таким образом, что исключена возможность случайного просмотра посетителями отображаемой на них информации.

Парольная авторизация входа пользователя ОИ в ЛВС осуществляется на всех АРМ ОИ.

В Таможенном управлении, в том числе на АРМ ОИ, используется антивирусная программа Kaspersky Endpoint Security 10 для Windows, сертифицированная по требованиям безопасности информации (сертификат ФСТЭК № 3025 действителен до 25.11.2019 г.).

Ответственные за безопасность информации в помещениях обследуемого ОИ не назначены. Документально регламентирован доступ в обследуемые помещения.

Основные технические средства (АРМ) обследуемого ОИ находятся на балансе Таможенного управления, но за пользователями документально не закреплены.

1.3.3. Программные средства защиты информации

На момент обследования были выявлены следующие средства защиты информации, их перечень указан в таблице 2. Все средства настроены корректно согласно инструкции.

Таблица 2 – Программно-аппаратные средства защиты

№ п/п	Наименование и тип технического средства	Заводской номер	Сведения о сертификате/№ лицензии	Место и дата установки
1	2	3	4	5
1.	СЗИ от НСД «Dallas Lock 7.5»	38160-3608-396 СЗЗ М229482	Сертификат ФСТЭК России: № 1685. Срок действия истек. Продление не планируется.	ПЭВМ №1-ПЭВМ №6 15.03.12

Продолжение таблицы 2

1	2	3	4	5
2.	Средство антивирусной защиты Kaspersky Endpoint Security 10 для Windows	17E0-00045104 EEF4C3B /Л866418	Сертификат ФСТЭК России № 3025 (от 25.11.2013 до 25.11.2019).	ПЭВМ№1-ПЭВМ №6 06.11.17
3.	Персональное средство аутентификации (электронный ключ) eToken	470BF614	Сертификат ФСТЭК России: № 1883 действителен до 11.08.2019 г	-
		47066914		
		47064A14		
		47063814		
		46A1D814		
		46FBFE14		
		470BF714		
		470BF712		
4.	АПКШ "Континент IPC-100"	G2UGEP87 /E828180	Сертификат ФСТЭК № 3008 действителен до 01.11.2019 г	-
		JF873TGY /Г641540		
		V2K8DPRY /Г641515		
		SJ8818VT /Г641509		
		4Z2ME1ZE /Г641527		

1.4. Организационно-распорядительные и нормативно-методические документы по защите информации

На настоящий момент в Таможенном управлении утверждены следующие документы по обеспечению безопасности конфиденциальной информации (в том числе персональных данных):

– акт классификации "ОПСУР";

– перечень защищаемых ресурсов "ОПСУР";

– журнал ознакомления должностных лиц с основами информационной безопасности в таможенных органах;

– инструкция о применении средств антивирусной защиты информации в Таможенном управлении;

– инструкция по проведению антивирусного контроля на рабочей станции в Таможенном управлении;

– инструкция по работе в АИС «ЕБВР»;

– приказ о назначении администраторов безопасности подсистемы криптографической защиты информации в Таможенном управлении;

– приказ о назначении постоянно действующей комиссии по категорированию и классификации выделенных помещений и автоматизированных рабочих мест;

– приказ о назначении администраторов безопасности межсетевого экранирования;

– политика обработки персональных данных в ИСПДн «ОПСУР»;

– порядок организации доступа должностным лицам таможни к информационным ресурсам Таможенного управления

– порядок учета, обращения и хранения конфиденциальной информации на машинных носителях информации;

– требования по обеспечению безопасности персональных данных в таможенных органах Российской Федерации, организациях, находящихся в ведении ФТС России, при их обработке в информационных системах персональных данных таможенных органов Российской Федерации;

– перечень персональных данных, обрабатываемых в таможенных органах Российской Федерации, организациях, находящихся в ведении ФТС России, представительствах (представителями) таможенной службы Российской Федерации в иностранных государствах в связи с реализацией служебных или трудовых отношений, перечня персональных данных, обрабатываемых в таможенных органах;

– положение о подсистеме антивирусной защиты информации таможенных органов;

– модель угроз по обеспечению с помощью криптосредств безопасности персональных данных;

– распоряжение об утверждении перечня пользователей средств криптографической защиты информации

– инструкция по организации и обеспечению безопасности эксплуатации шифровальных (криптографических) средств в информационных системах;

– инструкция ответственного пользователя за обращение со средствами криптографической защиты информации;

– инструкция пользователя шифровальных (криптографических) средств защиты информации;

– журнал учета средств криптографической защиты информации;

На момент обследования ИС функции, связанные с организацией и обеспечением защиты информации, возложены на администратора информационной безопасности информационных систем персональных данных. Администратор информационной безопасности назначен распоряжением начальника Таможенного управления.

Лицо, ответственное за организацию обработки персональных данных в Таможенном управлении не назначено.

1.5. Сведения о классификации ИСПДн

Согласно действующему акту классификации ИСПДн "ОПСУР", возможность возникновения угроз 1-го и 2-го типа, связанных с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении (далее – ПО), используемом в автоматизированной системе исключается ввиду отсутствия мотивации осуществления деятельности, связанной с нарушением характеристик безопасности информации у нарушителей, которые могут использовать данные уязвимости (разведывательные службы, разработчики операционных систем), а также отсутствия информации в ИСПДн, ценной для данных нарушителей. Остальные типы нарушителей, ввиду сложности и больших финансовых затрат для реализации уязвимостей не рассматриваются.

В соответствии с частью 6 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства РФ от 1 ноября 2012 г. № 1119, для ИСПДн актуальны угрозы 3-го типа, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном ПО, используемом в информационной системе.

Основываясь на порядке определения требуемого уровня защищенности, в соответствии с Постановлением Правительства Российской Федерации №1119 от 1 ноября 2012 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», для персональных данных, обрабатываемых в ИСПДн, необходимо обеспечить 4 (Четвертый) уровень защищенности.

1.6. Вывод по первой главе

При проведении обследования было определено соответствие текущего уровня защиты объекта информатизации ИСПДн «ОПСУР» Таможенного управления требованиям законодательства в сфере защиты информации.

Соответствие требованиям, предусмотренным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» представлено в таблице 3.

Таблица 3 – Соответствие требованиям ФЗ №152 от 27.07.06

Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»	Сведения о реализации мер
1	2
1. Назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных	Не реализовано
2. Издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений, в частности: правил обработки персональных данных, устанавливающих процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований; перечня персональных данных, обрабатываемых в ИСПДн (уровень защищенности, объем, сроки хранения) и подлежащих защите; перечня лиц осуществляющих обработку персональных данных (пользователи) и лиц имеющих доступ к персональным данным (ответственные лица, обслуживающих персонал); должностной инструкции ответственного за организацию обработки персональных данных.	Реализовано частично (отсутствует должностная инструкция, не актуализирован перечень лиц)

Продолжение таблицы 3

1	2
3. Применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных»: определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных; применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных; применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации; оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных; учет машинных носителей персональных данных; обнаружение фактов несанкционированного доступа к персональным данным и принятием мер; восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним; установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных; контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных.	Реализовано частично
4. Ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, и (или) организация обучения указанных лиц	Реализовано

Соответствие требованиям по обеспечения уровня защищенности персональных данных, утвержденных постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» представлено в таблице 4.

Таблица 4 – Соответствие требованиям ПП №1119 от 01.11.12

Требования для обеспечения 4-го уровня защищенности ПДн	Сведения о выполнении
1. Организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения	Выполнено
2. Обеспечение сохранности носителей персональных данных	Выполнено частично, нет учета носителей
3. Утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей	Не выполнено (не актуализирован)
4. Использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз	Выполнено частично. Сертификат на СЗИ от НСД утратил силу.

Соответствие требованиям, утвержденных приказом 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» представлено в таблице 5.

Таблица 5 – Соответствие требованиям приказа ФСТЭК №21 от 18.02.13

Организационные и технические меры по обеспечению безопасности персональных данных, которые должны быть реализованы в составе системы защиты	Сведения о реализации мер
1	2
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	Реализована средствами СЗИ от
II. Управление доступом субъектов доступа к объектам доступа (УПД)	

Продолжение таблицы 5

1	2
V. Регистрация событий безопасности (РСБ)	НСД утратившими сертификат
VI. Антивирусная защита (АВЗ)	Реализована
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)	Реализована средствами СЗИ от НСД утратившими сертификат
XI. Защита среды виртуализации (ЗСВ)	Не применимо
XII. Защита технических средств (ЗТС)	Реализована частично. СЗИ от НСД утратило сертификат
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	

Уменьшить вероятность реализации указанных угроз, вплоть до полного устранения некоторых из них, позволит модернизация системы защиты персональных данных объекта информатизации, которая должна предусматривать комплекс организационных, программно-технических средств мер по защите информации, при ее обработке на ОИ в соответствии с требованиями нормативных документов Российской Федерации в области защиты персональных данных.

На основании актуальных угроз безопасности информации для объекта информатизации Таможенного управления необходимо разработать детализированные требования к модернизации системы защиты персональных данных объекта информатизации.

2.ТЕОРЕТИЧЕСКОЕ ОБОСНОВАНИЕ РЕАЛИЗАЦИИ СРЕДСТВ И МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ

2.1. Анализ угроз

Для детализирования возможных методов и средств модернизации системы защиты информации, необходимо произвести анализ угроз и выявить среди них актуальные, составить модель нарушителя. Именно эти данные в дальнейшем определят основные пути и средства модернизации действующей системы защиты. Параллельно следует произвести актуализацию технических средств вычислительной техники, их окружение, расположение и линии коммуникаций. Чтобы оценить актуальность угрозы утечки информации по каналам побочных электромагнитных излучений и наводок(ПЭМИН) необходимо измерить расстояние, на которое распространяется информативный сигнал от всех ОТСС и выяснить выходит ли он за границу контролируемой зоны.

При проведении обследования был осуществлен замер ПЭМИН на всех ОТСС. На основании полученных данных был составлен протокол оценки защищенности объекта информатизации информационной системы персональных данных «ОПСУР» Таможенного управления на соответствие требованиям по защите информации от утечки по каналам ПЭМИН (Приложение А). В результате было выявлено, что информативный сигнал не выходит за пределы контролируемой зоны.

В ходе анализа данных и при использовании метода экспертной оценки существующих мер защиты, была составлена модель угроз (Приложение Б), включающая в себя также и модель нарушителя. В результате актуальными были выявлены следующие угрозы:

1. Подделка записей журнала регистрации событий.
2. Несанкционированное изменение параметров настройки средств защиты информации.
3. Доступ к защищаемым файлам с использованием альтернативных путей доступа к ресурсам.
4. Несанкционированная модификация защищаемой информации.
5. Несанкционированное удаление защищаемой информации.
6. Несанкционированный доступ к аутентификационной информации.
7. Несанкционированные изменения аутентификационной информации.
8. Удаление аутентификационной информации.
9. Угроза обхода некорректно настроенных механизмов аутентификации.
10. Несанкционированное создание учетной записи пользователей.
11. Угроза Несанкционированного использования системных и сетевых утилит.
12. Использование механизмов авторизации для повышения привилегий.
13. Несанкционированное редактирование реестра.
14. Некорректное использование функционала программного обеспечения.
15. Нарушение целостности данных кеша.

16. Обнаружение открытых портов и идентификации привязанных к ним сетевых служб.

17. Обнаружение хостов.

18. Определение типов объектов защиты и получение предварительной информации об объекте защиты.

19. Удаленный подбор аутентификационных данных пользователя.

20. Преднамеренное изменение или уничтожение программных компонентов ИС.

21. Внедрение программных закладок.

22. Подделка записей журнала регистрации событий.

23. Несанкционированное изменение параметров настройки средств защиты информации.

24. Несанкционированный доступ к информации с применением стандартных функций операционной системы (уничтожение, копирование, перемещение и т. п.).

25. Несанкционированный доступ к информации с использованием прикладного программного обеспечения.

26. Неправомерное ознакомление с защищаемой информацией.

27. Несанкционированная модификация защищаемой информации.

28. Несанкционированное копирование информации на внешние (сменные) носители.

29. Несанкционированный доступ к аутентификационной информации.

30. Несанкционированные изменения аутентификационной информации.

31. Удаление аутентификационной информации.

32. Угроза обхода некорректно настроенных механизмов аутентификации.

33. Использование механизмов авторизации для повышения привилегий.

34. Удаление защищаемой информации.

35. Несанкционированное восстановление удаленной защищаемой информации.

36. Несанкционированное создание учетной записи пользователей.

37. Несанкционированное редактирование реестра.

38. Повреждение системного реестра.

39. Угроза несанкционированного использования системных и сетевых утилит.

40. Несанкционированное повышение привилегий пользователя операционной системы.

41. Несанкционированное повышение привилегий пользователя.

На основе данных угроз были составлены требования к системе защиты информации (Приложение В).

2.2. Нейтрализация угроз.

2.2.1. Программно-аппаратные средства

Большая часть угроз вызвана отсутствием на АРМ сертифицированного СЗИ от НСД. На момент обследования на компьютерах был установлен Dallas Lock 7.5. Данное ПО имеет сертификат ФСТЭК России: № 1685, однако 18.09.2017 он утратил силу, и продление разработчик не планирует. Все пользователи ИС проинструктированы о работе с СЗИ, а администраторы ИС обучены настройке. Внутри СЗИ от НСД были прописаны персональные идентификаторы работников ИСПДн.

Связи со структурной реорганизацией Таможенного управления изменилось количество таможенных постов, а также было осуществлено упразднение одного из административных зданий, подведомственных Таможенному управлению. По этой причине высвободилось около 10 лицензий СЗИ от НСД Dallas Lock 8.0-C с модулями «Межсетевой экран» и «Система обнаружения вторжения», и именно их заказчик пожелал использовать при модернизации системы защиты ИСПДн «ОПСУР».

Характеристики Dallas Lock 8.0-C указаны в таблице 6.

Таблица 6 - Характеристики средства защиты

Характеристика	Удовлетворяемые требования
1	2
Сертификат ФСТЭК	№ 2945 от 16.08.2013г. Действителен до 16.08.2019 г.
Поддерживаемые ОС	Windows XP (SP 3) (Professional, Home, Starter); Windows Server 2003 (R2) (SP 2) (Web, Standard, Enterprise, Datacenter); Windows Vista (SP 2) (Ultimate, Enterprise, Business, Home Premium, Home Basic, Starter); Windows Server 2008 (SP 2) (Standard, Enterprise, Datacenter, Web Server 2008, Storage Server 2008); Windows 7 (SP 1) (Ultimate, Enterprise, Professional, Home Premium, Home Basic, Starter); Windows Server 2008 R2 (SP 1) (Foundation, Standard, Web, Enterprise, Datacenter); Windows 8 (Core, Pro, Enterprise); Windows Server 2012 (Foundation, Essentials, Standard, Datacenter); Windows 8.1 (Core, Pro, Enterprise); Windows Server 2012 (R2) (Foundation, Essentials, Standard, Datacenter); Windows 10 (Enterprise, Education, Pro, Home) и Windows 10 Creators Update; Windows Server 2016.

Продолжение таблицы 6

1	2
Класс защищенности АС	1Б включительно (Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации» (Гостехкомиссия России, 1992));
Уровень защищенности ИСПДн	1 уровень (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»);
Межсетевое экранирование	до 1В включительно
Средство обнаружения вторжения	до 1Г включительно
Класс автоматизированных систем	до 1Б включительно
Поддерживаемые аппаратные идентификаторы	USB-Flash-накопители; электронные ключи Touch Memory (iButton); USB-ключи и смарт-карты eToken; USB-ключи Рутокен; USB-ключи и смарт-карты JaCarta; карты HID Proximity; USB-ключи и смарт-карты ESMART.

Таким образом Dallas Lock 8.0-C удовлетворяет всем необходимым требованиям для использования в системе защиты ИСПДн «ОПСУР».

Антивирусная защита реализована на базе Kaspersky Endpoint Security 10 для Windows, сертифицированная по требованиям безопасности информации (сертификат ФСТЭК № 3025 действителен до 25.11.2019 г.). Так как сертификат и лицензия на момент обследования действовали, то замена средства защиты не требуется.

Передача защищаемой информации через средства и системы связи общего пользования (Интернет) осуществляется через сертифицированное средство криптографической зашиты информации – аппаратно-программный комплекс шифрования (АПКШ) «Континент». Такой комплекс стоит на каждой логической ветви ЛВС. Средство имеет сертификат ФСТЭК № 3008 действующий до 01.11.2019 г. Модернизация не требуется.

2.2.2. Организационные меры

Все организационные меры защиты заключаются в устранении несоответствия организационно распорядительной документации Таможенного управления требованиям законодательства путем ее дополнения.

В соответствии с ФЗ №152 от 27.07.06 в Таможенном управлении на данный момент не выполнены следующие требования:

– Не назначен ответственный за организацию обработки персональных данных

– Отсутствует должностная инструкция ответственного за организацию обработки персональных данных.

– Нет актуального перечня лиц, осуществляющих обработку персональных данных (пользователи) и лиц, имеющих доступ к персональным данным (ответственные лица, обслуживающих персонал);

– Не выполнено применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

В соответствии с ПП от 01.11.12 г. № 1119 в Таможенном управлении на данный момент не выполнены следующие требования:

– Отсутствует учет носителей защищаемой информации;

– Не актуализирован перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

Для устранения выявленных недостатков необходимо дополнить организационно-распорядительную документацию.

2.3. Вывод по второй главе

В результате анализа угроз безопасности информации в ИСПДн «ОПСУР» Таможенного управления были выявлены основные направления модернизации текущей системы защиты.

Большая часть угроз связана с отсутствуем на АРМ сертифицированного средства защиты от НСД. Нейтрализацией данных угроз выступает установка и настройка сертифицированного СЗИ от НСД Dallas Lock 8.0-С.

Угрозы утечки информации по каналам ПЭМИН, по результатам замеров, признаны неактуальными – информативный сигнал не выходит за пределы контролируемой зоны.

Видовая информация защищена достаточно – работники проинструктированы о работе с защищаемой информацией в присутствии посторонних лиц, мониторы ПЭВМ расположены таким образом, что исключено случайное или намеренное подглядывание. На окнах установлены шторы или жалюзи.

Анализ организационно-распорядительной документации показал необходимость ее дополнения следующими сведениями:

– Назначение ответственного за обработку ПДн;

– права и обязанности ответственного за обработку ПДн;

– перечень должностей служащих и работников Таможенного управления, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;

– перечень лиц, допущенных к обработке персональных данных в ИСПДн «ОПСУР» Таможенного управления;

– организация учета, использования и уничтожения носителей персональных данных в Таможенном управлении;

– инструкция по настройке СЗИ.

3. МОДЕРНИЗАЦИЯ ЗАЩИТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ «ОПСУР»

3.1. Общая информация

В результате проведенного обследования текущего состояния системы защиты информации ИСПДн «ОПСУР» Таможенного управления, выявленных актуальных угроз, а также в ходе анализа путей их нейтрализации, были определены основные направления модернизации системы защиты.

Для нейтрализации угроз НСД производится установка и настройка СЗИ от НСД Dallas Lock 8.0-C;

Для устранения выявленных недостатков по части организационно-распорядительной документации, её дополнили следующими документами:

1. инструкция лица, ответственного за организацию обработки персональных данных в Таможенном управлении (Приложение Г);
2. перечень должностей служащих и работников Таможенного управления, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;
3. перечень лиц, допущенных к обработке персональных данных в ИСПДн «ОПСУР» Таможенного управления;
4. инструкция по организации учета, использования и уничтожения носителей персональных данных в Таможенном управлении (Приложение Д);

На основании обновленных сведений также был составлен технический паспорт (Приложение Е).

3.2. Стадии реализации

Стадии работ по модернизации СЗИ, соответствующие, и сроки их выполнения приведены в таблице 7.

Таблица 7 – Стадии по созданию СЗИ и сроки их выполнения.

Стадия работ	Описание	Срок выполнения
1	2	3
Техническое задание	На данной стадии производится разработка, согласование и утверждение технического задания на создание СЗИ.	Стадия завершена
Технорабочий проект	На данной стадии производится разработка проектных решений по СЗИ.	-

Продолжение таблицы 7

1	2	3
Ввод в действие	На данной стадии производится выполнение следующих этапов: разработка документации на СЗИ; адаптация и настройка системы; пусконаладочные работы; проведение предварительных испытаний; проведение опытной эксплуатации; проведение приёмочных испытаний.	Срок выполнения стадии определяется соответствующими договорами между Заказчиком и организациями-исполнителями работ
Сопровождение СЗИ	На данной стадии производится выполнение работ в соответствии с гарантийными обязательствами.	Срок выполнения стадии определяется соответствующими договорами между Заказчиком и организациями-исполнителями работ.

3.3. Основные технические решения

3.3.1. Архитектурные решения СЗИ

Организация системы защиты информации представляет собой комплекс организационных и технических мероприятий.

Архитектура СЗИ разрабатывается на основании требований технического задания на комплекс мероприятий по построению системы защиты информации ИС.

Согласно ТЗ, в системе защиты информации, должны быть приняты следующие меры по обеспечению безопасности информации:

а) идентификация и аутентификация субъектов доступа и объектов доступа;

б) управление доступом субъектов доступа к объектам доступа;

в) ограничение программной среды;

г) защита машинных носителей информации;

д) регистрация событий безопасности;

е) антивирусная защита;

ж) контроль (анализ) защищенности информации;

з) обеспечение целостности информационной системы и информации;

и) обеспечение доступности информации;

к) защита технических средств.

На АРМ ИС предлагается к использованию сертифицированная система защиты информации от несанкционированного доступа «Dallas Lock 8.0-C».

В целях организации двухфакторной аутентификации предлагается использовать электронные ключи RuToken.

В качестве средства антивирусной защиты информации предлагается к использованию имеющееся у Заказчика сертифицированное ПО Kaspersky Endpoint Security 10.

Организационно-технические меры защиты информации от несанкционированного доступа включают:

– обеспечение физической защиты помещения, в котором установлены технические средства ИС;

– регламентирование доступа лиц в помещение, в котором установлены технические средства ИС;

– регламентирование действия сотрудников (пользователей, администратора и обслуживающего персонала), имеющих доступ к АРМ ИС;

– организацию учета и использования машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;

3.3.2. Применяемые средства защиты информации

3.3.2.1. Система защиты информации от несанкционированного доступа «Dallas Lock 8.0-C»

Система защиты информации от несанкционированного доступа «Dallas Lock 8.0-C» соответствует требованиям руководящих документов «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» - по 2 уровню контроля и «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» - по 3 классу защищенности. Сертификат ФСТЭК России №2945 действителен до 16.08.2019 г.

Функциональные возможности СЗИ от НСД Dallas Lock 8.0-C:

В соответствии со своим назначением СЗИ от НСД Dallas Lock 8.0-C запрещает посторонним лицам доступ к ресурсам ПК и позволяет разграничить права пользователей при работе на компьютере. Разграничения касаются прав доступа к объектам файловой системы, к устройствам, прав доступа к сети, сменным накопителям, аппаратным ресурсам. Для облегчения администрирования возможно объединение пользователей в группы. Контролируются права доступа для локальных, доменных, сетевых и терминальных пользователей.

Для предотвращения утечки информации с использованием сменных накопителей (таких как CD-диск, USB-Flash-диск и прочие) СЗИ от НСД обеспечивает следующие функции:

1) разграничение доступа к типам накопителей и к конкретным экземплярам;

2) преобразование сменных накопителей с использованием ключа (используется криптоалгоритм, пароль и (или) аппаратный идентификатор);

3) создание теневых копий файлов, отправляемых на сменные или сетевые накопители.

СЗИ от НСД Dallas Lock 8.0-C позволяет в качестве средства опознавания пользователей использовать электронные идентификаторы. Дополнительно имеется возможность определения принадлежности аппаратного идентификатора.

Для решения проблемы «простых» паролей СЗИ от НСД имеет гибкие настройки их сложности. Для создания пароля, соответствующего всем установленным настройкам, в СЗИ от НСД реализована функция генерации паролей.

В Dallas Lock 8.0-C реализован контроль доступа пользователей к объектам файловой системы (дискам, папкам и файлам под FAT и NTFS). Применяется полностью независимый от ОС механизм. Используются дискреционный принцип контроля доступа: обеспечивается доступ к защищаемым объектам (дискам, каталогам, файлам, устройствам) в соответствии со списками пользователей (групп) и их правами доступа (матрица доступа).

В Dallas Lock 8.0-C реализован контроль доступа к подключаемым (не системным) устройствам: возможность разграничения доступа и аудит событий доступа. Список устройств отображается в виде дерева объектов, которое содержит классы устройств и индивидуальные устройства.

В Dallas Lock 8.0-C реализована функция «Изолированные процессы», которая позволяет исключить возможность копирования информации через буфер обмена средствами терминального подключения к удалённому компьютеру.

В СЗИ от НСД Dallas Lock 8.0-C реализована система контроля целостности параметров компьютера, которая обеспечивает:

1) контроль целостности программно-аппаратной среды при загрузке компьютера, по расписанию, через заданные интервалы (периодический контроль) и по команде администратора;

2) контроль целостности объектов ФС (файлов и папок) при загрузке компьютера, по расписанию, через заданные интервалы (периодический контроль) и по команде администратора;

3) контроль целостности веток реестра при загрузке компьютера, по расписанию, через заданные интервалы (периодический контроль) и по команде администратора;

4) блокировку входа в ОС компьютера при выявлении нарушения целостности;

5) проверку целостности объектов ФС (файлов и папок) при доступе;

6) восстановление файла в случае обнаружения нарушения его целостности.

СЗИ от НСД Dallas Lock 8.0-Свключает подсистему очистки остаточной информации, которая гарантирует предотвращение восстановления удаленных данных. Специальные политики определяют количество циклов очистки: 1, 2

или 3; производится ли очистка для всех или только конфиденциальных данных. Зачистка дискового пространства производится либо по команде пользователя, либо в автоматическом режиме.

В СЗИ от НСД Dallas Lock 8.0-C реализована функция «Зачистка диска», которая позволяет полностью зачищать остаточные данные всего диска или его разделов. Это может быть полезно при снятии носителей с учета и необходимости полного удаления данных без возможности их восстановления по остаточной информации.

В СЗИ от НСД Dallas Lock 8.0-C реализовано ведение 6 электронных журналов, в которых фиксируются действия пользователей:

1) журнал входов;
2) журнал управления учетными записями;
3) журнал ресурсов;
4) журнал печати;
5) журнал управления политиками;
6) журнал процессов.

Для защиты данных при хранении их на сменных носителях либо при передаче по различным каналам связи имеется возможность преобразования данных в файл-контейнер с помощью криптопровайдера. В качестве ключа преобразования используется пароль и (или) аппаратный идентификатор.

Dallas Lock 8.0-C позволяет настраивать «Замкнутую программную среду» (ЗПС), режим, в котором пользователь может запускать только программы, определенные администратором.

Для удобства администрирования СЗИ от НСД, возможно задание списка расширений файлов, работа с которыми будет блокирована.

Предусматривается ведение резервных копий программных средств защиты информации, их периодическое обновление и контроль работоспособности, а также возможность возврата к настройкам по умолчанию.

3.3.2.2. ПО Kaspersky Endpoint Security 10 для Windows

ПО Kaspersky Endpoint Security 10 для Windows является средством антивирусной защиты, соответствует требованиям документов «Требования к средствам антивирусной защиты» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа Б второго класса защиты. ИТ.САВ3.Б2.ПЗ» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа В второго класса защиты. ИТ.САВ3.В2.ПЗ» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа Г второго класса защиты. ИТ.САВ3.Г2.ПЗ» (ФСТЭК России, 2012). Сертификат ФСТЭК №3509, действителен до 25.11.2019 г.

Kaspersky Endpoint Security обеспечивает комплексную защиту компьютера от известных и новых угроз, сетевых и мошеннических атак. Каждый тип угроз

обрабатывается отдельным компонентом. Компоненты можно включать и выключать независимо друг от друга, а также настраивать параметры их работы.

К компонентам контроля относятся следующие компоненты программы:

1) Контроль запуска программ. Компонент отслеживает попытки запуска программ пользователями и регулирует запуск программ.

2) Контроль активности программ. Компонент регистрирует действия, совершаемые программами в операционной системе, и регулирует деятельность программ исходя из того, к какой группе компонент относит эту программу. Для каждой группы программ задан набор правил. Эти правила регламентируют доступ программ к персональным данным пользователя и ресурсам операционной системы. К таким данным относятся файлы пользователя (папка «Мои документы», файлы cookie, данные об активности пользователя), а также файлы, папки и ключи реестра, содержащие параметры работы и важные данные наиболее часто используемых программ.

3) Мониторинг уязвимостей. Мониторинг уязвимостей в режиме реального времени проверяет программы, запущенные на компьютере пользователя, а также проверяет программы в момент их запуска.

4) Контроль устройств. Компонент позволяет установить гибкие ограничения доступа к устройствам, являющимся источниками информации (например, жесткие диски, съемные носители информации, ленточные накопители, CD/DVD-диски), инструментами передачи информации (например, модемы), инструментами превращения информации в твердую копию (например, принтеры) или интерфейсами, с помощью которых устройства подключаются к компьютеру (например, USB, Bluetooth, Infrared).

3.3.3. Подсистема организационно-правовых мероприятий

Подсистема организационно-правовых мероприятий обеспечивает создание правовой, организационной и методической основы для функционирования СЗИ и включает в себя следующие виды документов:

– акт классификации "ОПСУР";

– перечень защищаемых ресурсов "ОПСУР";

– журнал ознакомления должностных лиц с основами информационной безопасности в таможенных органах;

– инструкция о применении средств антивирусной защиты информации в Таможенном управлении;

– инструкция по проведению антивирусного контроля на рабочей станции в Таможенном управлении;

– инструкция по работе в АИС «ЕБВР»;

– приказ о назначении администраторов безопасности подсистемы криптографической защиты информации в Таможенном управлении;

– приказ о назначении постоянно действующей комиссии по категорированию и классификации выделенных помещений и автоматизированных рабочих мест;

– приказ о назначении администраторов безопасности межсетевого экранирования;

– порядок организации доступа должностным лицам таможни к информационным ресурсам Таможенного управления

– порядок учета, обращения и хранения конфиденциальной информации на машинных носителях информации;

– политика обработки персональных данных в ИСПДн «ОПСУР»;

– требования по обеспечению безопасности персональных данных в таможенных органах Российской Федерации, организациях, находящихся в ведении ФТС России, при их обработке в информационных системах персональных данных таможенных органов Российской Федерации;

– перечень персональных данных, обрабатываемых в таможенных органах Российской Федерации, организациях, находящихся в ведении ФТС России, представительствах (представителями) таможенной службы Российской Федерации в иностранных государствах в связи с реализацией служебных или трудовых отношений, перечня персональных данных, обрабатываемых в таможенных органах;

– инструкция лица, ответственного за организацию обработки персональных данных в Таможенном управлении;

– перечень должностей служащих и работников Таможенного управления, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;

– перечень лиц, допущенных к обработке персональных данных в ИСПДн «ОПСУР» Таможенного управления;

– инструкция по организации учета, использования и уничтожения носителей персональных данных в Таможенном управлении;

– положение о подсистеме антивирусной защиты информации таможенных органов.

– модель угроз по обеспечению с помощью криптосредств безопасности персональных данных;

– распоряжение об утверждении перечня пользователей средств криптографической защиты информации

– инструкция по организации и обеспечению безопасности эксплуатации шифровальных (криптографических) средств в информационных системах;

– инструкция ответственного пользователя за обращение со средствами криптографической защиты информации;

– инструкция пользователя шифровальных (криптографических) средств защиты информации;

– журнал учета средств криптографической защиты информации;

3.3.4. Идентификация и аутентификация субъектов доступа и объектов доступа

Для реализации требований к 4 уровню защищенности персональных данных, необходимо обеспечить следующие меры:

а) идентификация и аутентификация пользователей, являющихся работниками оператора;

б) управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов;

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

г) защита обратной связи при вводе аутентификационной информации.

Для реализации вышеуказанных требований на ПЭВМ пользователей должно быть установлено средство защиты информации от НСД «Dallas Lock 8.0-C».

Настройки механизмов безопасности СЗИ от НСД «Dallas Lock 8.0-C» обеспечивают защиту технических средств ИС от несанкционированного доступа.

СЗИ от НСД «Dallas Lock 8.0-C» должно быть установлено в необходимой комплектности в соответствии паспортом на изделие. Настройка средств защиты должна быть произведена в соответствии с документацией на систему, без нарушений.

В соответствии с действующей на объекте информатизации разрешительной системой допуска в ИС средствами СЗИ от НСД «Dallas Lock 8.0-C» и должны быть реализованы правила доступа, при которых каждый пользователь в соответствии с назначенными правилами имеет доступ:

а) к средствам ОС, обеспечивающим запуск и функционирование ИС;

б) к средствам антивирусной защиты;

в) к программным средствам, установленным на ПЭВМ;

г) к портам системного блока;

д) к средствам настройки системы защиты;

е) к устройствам ПЭВМ.

Порядок хранения, выдачи, инициализации, блокирования средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации в Таможенном управлении должен регламентироваться.

В ИС должна быть реализована двухфакторная аутентификация средствами СЗИ от НСД «Dallas Lock 8.0-C» с использованием персональных идентификаторов RuToken.

3.3.5. Управление доступом субъектов доступа к объектам доступа

Для реализации требований к 4 уровню защищенности персональных данных, необходимо обеспечить следующие меры:

а) управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей;

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

в) разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы;

г) назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы;

д) ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе);

е) блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу;

ж) разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации.

Управление учетными записями пользователей должен осуществлять администратор безопасности ИС посредством СЗИ от НСД «Dallas Lock 8.0-C», путем создания, активации, блокирования и уничтожения учетных записей пользователей ИС.

Настройка системы защиты должна обеспечить реализацию дискреционного метода контроля доступа – доступ к защищаемым объектам (дискам, каталогам, файлам) в соответствии со списками пользователей (групп) и их правами доступа. В соответствии с содержимым списка вычисляются права на доступ к объекту для каждого пользователя (открытие, запись, чтение, удаление, переименование, запуск, копирование). Настройками системы защиты обеспечивается автоматическое блокирование сеанса доступа в ИС после осуществления 5 неуспешных попыток входа в ИС или 15 минут бездействия (неактивности) пользователей.

Полномочия (роли) администраторов ИС и пользователей ИС должны быть назначены в соответствии с выполняемыми должностными обязанностями. Должны быть назначены минимально необходимые права и привилегии пользователям, администраторам и лицам, обеспечивающим функционирование ИС.

3.3.6. Ограничение программной среды

Для реализации требований к 4 уровню защищенности персональных данных, необходимо обеспечить установку (инсталляцию) только разрешенного к использованию программного обеспечения и (или) его компонентов.

Контроль состава установленного ПО должен осуществляется администратором ИС на периодической основе.

Средствами СЗИ от НСД «Dallas Lock 8.0-C» должен быть реализован запрет на установку, деинсталляцию и изменение программного обеспечения в составе ИС. Установка компонентов программного обеспечения должна осуществляться исключительно администратором ИС.

Установка средств защиты информации должна осуществляться администратором информационной безопасности ИС с сертифицированного дистрибутива, входящего в комплект поставки СЗИ.

3.3.7. Защита машинных носителей информации

Для реализации требований к 4 уровню защищенности персональных данных, необходимо обеспечить следующие меры:

а) учет машинных носителей информации;

б) управление доступом к машинным носителям информации;

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

Все машинные носители, участвующие в процессе обработки информации в ИС должны быть учтены в «Журнале учета машинных носителей информации…».

Настройка механизма «Контроля устройств» СЗИ от НСД «Dallas Lock 8.0-C» должна обеспечить ограничение доступа пользователей ИС к машинным носителям информации и интерфейсам ввода (вывода) информации на машинные носители информации. Доступ к интерфейсам ввода (вывода) информации на машинные носители информации должен быть разрешен только тем пользователям ИС, для которых использование машинных носителей информации необходимо для выполнения технологического процесса обработки информации в ИС.

Настройка подсистемы очистки остаточной информации СЗИ от НСД «Dallas Lock 8.0-C» должна обеспечить принудительное уничтожение информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации.

3.3.8. Регистрация событий безопасности

Для реализации требований к 4 уровню защищенности персональных данных, необходимо обеспечить следующие меры:

а) определение событий безопасности, подлежащих регистрации, и сроков их хранения;

б) определение состава и содержания информации о событиях безопасности, подлежащих регистрации;

в) сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;

г) реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти;

д) мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них;

е) генерирование временных меток и (или) синхронизация системного времени в информационной системе;

ж) защита информации о событиях безопасности.

Для реализации вышеуказанных требований должна быть настроена подсистема регистрации и учета СЗИ от НСД «Dallas Lock 8.0-C», путем включения следующих параметров аудита:

а) журнал входов в систему;

б) журнал ресурсов;

в) журнал управления политиками безопасности

г) журнал управления учетными записями;

д) журнал запуска/завершения процессов;

е) аудит устройств;

ж) аудит доступа: Заносить в журналы ошибки Windows;

з) заносить в журнал события запуска и остановки ОС.

В СЗИ от НСД «Dallas Lock 8.0-C» должен быть настроен аудит доступа к ресурсам в системе защиты отдельно для глобальных параметров (вкладка «Контроль ресурсов» - категория «Глобальные»), и при необходимости отдельно для локальных объектов (вкладка «Контроль ресурсов» - категория «Аудит»). Аудит событий настраивается по принципу назначения дескриптора аудита для объекта, для этого в дескрипторе объекта имеется закладка «Аудит доступа» со списком операций, которые могут быть запротоколированы в системе защиты.

Доступ к параметрам аудита СЗИ от НСД «Dallas Lock 8.0-C должен быть разрешен только администратору информационной безопасности ИС.

Регистрация действий пользователей ИС в процессе работы в прикладном программном обеспечении осуществляется встроенными механизмами регистрации такого ПО.

3.3.9. Антивирусная защита

Для ИС на данный момент реализована антивирусная защита и обеспечено обновление базы данных признаков вредоносных компьютерных программ (вирусов).

Антивирусная защита информации обеспечивается средствами сертифицированного ПО Kaspersky Endpoint Security 10 для Windows. Установка антивирусного ПО должна произведена с сертифицированного ФСТЭК дистрибутива.

Обновление антивирусного ПО осуществляется администратором информационной безопасности ИС вручную.

Использование средств антивирусной защиты осуществляется в соответствии с «Инструкцией по организации антивирусной защиты…».

3.3.10. Контроль (анализ) защищенности информации

Для реализации требований к 4 уровню защищенности персональных данных, необходимо обеспечить:

а) контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации;

б) контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации;

в) контроль состава технических средств, программного обеспечения и средств защиты информации;

г) контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе.

Контроль установки обновлений ПО, работоспособности ПО, состава технических средств в составе ИС, должен осуществляться на периодической основе администратором ИС, но не реже одного раза в квартал.

Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе осуществляет администратор информационной безопасности ИС.

Результаты проведения контроля должны отражаться в Журнале учета мероприятий по контролю обеспечения защиты информации при ее обработке в ИС.

3.3.11. Обеспечение целостности информационной системы и информации

Для ИС необходимо обеспечение возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций.

Восстановление программного обеспечения при возникновении нештатных ситуаций должно осуществляться с дистрибутивов ПО администратором ИС и резервных копий.

3.3.12. Обеспечение доступности информации

Для реализации требований к 4 уровню защищенности персональных данных необходимо обеспечить:

а) периодическое резервное копирование информации на резервные машинные носители информации;

б) обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течении установленного временного интервала.

Все критически важные объекты ИС должны быть подключены к источникам бесперебойного питания.

3.3.13. Защита технических средств

Для реализации требований к 4 уровню защищенности персональных данных необходимо обеспечить:

а) определить границы контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования.

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

в) обеспечить размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.

3.4. Мероприятия по подготовке к вводу СЗИ в действие

Мероприятия по обучению и проверке квалификации персонала:

а) проведение мероприятий по обучению и проверке квалификации администратора безопасности ИС по установке и эксплуатации средств защиты информации;

б) проведение мероприятий по обучению пользователей ИС по работе с персональным компьютером, используемым программным обеспечением, с персональными данными;

в) проверка квалификации администратора информационной безопасности ИС и пользователей ИС в области обработки и обеспечения защиты персональных данных.

Мероприятия по созданию необходимых подразделений и рабочих мест:

а) назначение лица, ответственного за организацию обработки персональных данных в Таможне;

б) назначение администратора ИС;

в) назначение администратора безопасности ИС.

Мероприятия по изменению объекта автоматизации:

а) установка и настройка СЗИ от НСД «Dallas Lock 8.0-C»;

б) проверка работоспособности и опытная эксплуатация средств защиты информации.

3.5. Организационно-технические меры защиты информации от несанкционированного доступа

Меры включают в себя:

а) обеспечение физической защиты помещения, в котором установлены технические средства ИС;

б) регламентирование доступа лиц в помещение, в котором установлены технические средства И

в) размещение АРМ в условиях контролируемого доступа;

г) расположение мониторов АРМ таким образом, чтобы препятствовать возможности несанкционированного визуального съема информации с них;

д) организацию учета и использования машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;

е) регламентирование действия сотрудников (пользователей, администратора и обслуживающего персонала), имеющих доступ к АРМ в состав ИС.

3.6. Вывод по третей главе

В ходе модернизации защиты информационной системы персональных данных Таможенного управления были устранены все недостатки существующей системы защиты.

Для нейтрализации угроз НСД предлагается установка и настройка СЗИ от НСД Dallas Lock 8.0-C. В главе также расписаны основные компоненты и функции предлагаемого средства защиты информации.

Антивирусная защита не претерпела изменений и обеспечивается средствами сертифицированного ПО Kaspersky Endpoint Security 10 для Windows. Установка антивирусного ПО произведена с сертифицированного ФСТЭК дистрибутива.

Для устранения выявленных недостатков по части организационно-распорядительной документации, её дополнили следующими документами:

1. инструкция лица, ответственного за организацию обработки персональных данных в Таможенном управлении (Приложение Г);

2. перечень должностей служащих и работников Таможенного управления, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;

3. перечень лиц, допущенных к обработке персональных данных в ИСПДн «ОПСУР» Таможенного управления;

4. инструкция по организации учета, использования и уничтожения носителей персональных данных в Таможенном управлении (Приложение Д);

На основании обновленных сведений также был составлен технический паспорт (Приложение Е).

В главе также рассмотрены мероприятия необходимые для реализации:

– контроля (анализа) защищенности информации,

– обеспечения целостности информационной системы и информации

– обеспечения доступности информации

– защиты технических средств

– мероприятий по подготовке к вводу СЗИ в действие

– организационно-технической защиты информации от несанкционированного доступа

Вся представленная информация позволяет произвести модернизацию действующей системы защиты в рамках, удовлетворяющих требованиям законодательства.

4. БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

4.1. Введение

Правильная организация рабочего пространства сотрудника является залогом его успешной и продолжительной службы. Наиболее продолжительный аспект работы в Таможенном управлении связан с взаимодействием с информационной системой посредствам вычислительной техники, по этой причине важно обеспечить соответствие рабочих мест сотрудников действующим нормам стандартов по безопасности жизнедеятельности. Реализация требований санитарных правил позволит предотвратить неблагоприятное влияния на здоровье человека вредных факторов производственной среды и трудового процесса при работе с ПЭВМ.

4.2. Общие требования к организации рабочих мест пользователей

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

1. При размещении рабочих мест с ПЭВМ расстояние между рабочими столами с видеомониторами (в направлении тыла поверхности одного видеомонитора и экрана другого видеомонитора), должно быть не менее 2,0 м, а расстояние между боковыми поверхностями видеомониторов - не менее 1,2 м;
2. Рабочие места с ПЭВМ при выполнении творческой работы, требующей значительного умственного напряжения или высокой концентрации внимания, рекомендуется изолировать друг от друга перегородками высотой 1,5 - 2,0 м;
3. Экран видеомонитора должен находиться от глаз пользователя на расстоянии 600 - 700 мм, но не ближе 500 мм с учетом размеров алфавитно-цифровых знаков и символов;
4. Конструкция рабочего стола должна обеспечивать оптимальное размещение на рабочей поверхности используемого оборудования с учетом его количества и конструктивных особенностей, характера выполняемой работы. При этом допускается использование рабочих столов различных конструкций, отвечающих современным требованиям эргономики. Поверхность рабочего стола должна иметь коэффициент отражения 0,5 - 0,7;
5. Конструкция рабочего стула (кресла) должна обеспечивать поддержание рациональной рабочей позы при работе на ПЭВМ, позволять изменять позу с целью снижения статического напряжения мышц шейно-плечевой области и спины для предупреждения развития утомления. Тип рабочего стула (кресла) следует выбирать с учетом роста пользователя, характера и продолжительности работы с ПЭВМ. Рабочий стул (кресло) должен быть подъемно-поворотным, регулируемым по высоте и углам наклона сиденья и спинки, а также расстоянию спинки от переднего края сиденья, при этом регулировка каждого параметра должна быть независимой, легко осуществляемой и иметь надежную фиксацию;

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

7. Высота рабочей поверхности стола для взрослых пользователей должна регулироваться в пределах 680 - 800 мм; при отсутствии такой возможности высота рабочей поверхности стола должна составлять 725 мм;

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

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

10. Конструкция рабочего стула должна обеспечивать:

- Ширину и глубину поверхности сиденья не менее 400 мм;
- Поверхность сиденья с закругленным передним краем;
- Регулировку высоты поверхности сиденья в пределах 400 - 550 мм и углам наклона вперед до 15 град, и назад до 5 град.;
- Высоту опорной поверхности спинки 300 +-20 мм, ширину - не менее 380 мм и радиус кривизны горизонтальной плоскости - 400 мм;
- Угол наклона спинки в вертикальной плоскости в пределах +-30 градусов;
- Регулировку расстояния спинки от переднего края сиденья в пределах 260 - 400 мм;
- Стационарные или съемные подлокотники длиной не менее 250 мм и шириной - 50 - 70 мм;
- регулировку подлокотников по высоте над сиденьем в пределах 230 +-30 мм и внутреннего расстояния между подлокотниками в пределах 350 -500 мм;

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

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

4.3. Требования к помещениям для размещения рабочего места

При работе с вычислительной техникой важным фактором, обеспечивающим высокий уровень работоспособности, является правильно спроектированное

помещение в котором будут располагаться рабочие места, оборудование ЭВМ с ВДТ.

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

1. Помещения для эксплуатации ПЭВМ должны иметь естественное и искусственное освещение;
2. Естественное и искусственное освещение должно соответствовать требованиям действующей нормативной документации. Оконные проемы должны быть оборудованы регулируемыми устройствами типа: жалюзи, занавесей, внешних козырьков и др.;
3. Площадь на одно рабочее место пользователей ПЭВМ с ВДТ на базе плоских дискретных экранов (жидкокристаллические, плазменные), должна составлять не менее 4,5 $м^2$;
4. 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;
5. Помещения, где размещаются рабочие места с ПЭВМ, должны быть оборудованы защитным заземлением (занулением) в соответствии с техническими требованиями по эксплуатации;
6. Не следует размещать рабочие места с ПЭВМ вблизи силовых кабелей и вводов, высоковольтных трансформаторов, технологического оборудования, создающего помехи в работе ПЭВМ.

4.4. Требования к уровням шума на рабочих местах

Уровень шума на рабочих местах, при выполнении основных и вспомогательных производственных работ с использованием ПЭВМ не должен превышать показателей, устанавливаемых нормами СанПиН 2.2.2/2.4.1340-03 предельно допустимых значений для данных видов работ в соответствии с действующими санитарно-эпидемиологическими нормативами. А именно должен соответствовать нормам СанПиН 2.2.4.3359-16 для высококвалифицированной работы, требующей сосредоточенности, в рабочих комнатах. Источниками шума в данной организации являются рабочие станции и сервер. На основании СанПиН 2.2.4.3359-16, нормативным эквивалентным уровнем звука на рабочих местах является 80 дБА. В соответствии с нормами, ограничивающими предельно допустимое звуковое давление для рабочих мест, оснащенных ПЭВМ: шумящее оборудование, уровни шума которого превышают нормативные, должно размещаться вне помещений ПЭВМ.

4.5. Требования к освещению на рабочих местах

При работе с вычислительной техникой важным фактором, обеспечивающим высокий уровень работоспособности, является правильно спроектированное освещение, не вызывающее раннего переутомления.

Согласно СанПиН 2.2.2/2.4.1340-03, есть следующие требования к освещению на рабочих местах:

1. Рабочие столы следует размещать таким образом, чтобы видеодисплейные терминалы были ориентированы боковой стороной к световым проемам, чтобы естественный свет падал преимущественно слева;
2. 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, следует применять системы комбинированного освещения;
3. Освещенность на поверхности стола в зоне размещения рабочего документа должна быть 300 - 500 лк. Освещение не должно создавать бликов на поверхности экрана. Освещенность поверхности экрана не должна быть более 300 лк;
4. Следует ограничивать прямую блесткость от источников освещения, при этом яркость светящихся поверхностей (окна, светильники и др.), находящихся в поле зрения, должна быть не более 200 кд/м.
5. Яркость светильников общего освещения в зоне углов излучения от 50 до 90° с вертикалью в продольной и поперечной плоскостях должна составлять не более 200 кд/м , защитный угол светильников должен быть не менее 40°.
6. Общее освещение при использовании люминесцентных светильников следует выполнять в виде сплошных или прерывистых линий светильников, расположенных сбоку от рабочих мест, параллельно линии зрения пользователя при рядном расположении видеодисплейных терминалов. При периметральном расположении компьютеров линии светильников должны располагаться локализовано над рабочим столом ближе к его переднему краю, обращенному к оператору;
7. Коэффициент пульсации не должен превышать 5%;
8. Для обеспечения нормируемых значений освещенности в помещениях для использования ПЭВМ следует проводить чистку стекол оконных рам и светильников не реже двух раз в год и проводить своевременную замену перегоревших ламп.

4.6. Требования к микроклимату

Для рабочих мест, на которых работа с ПЭВМ является основным видом выполняемых работ и связана с непрерывным эмоциональным напряжением, согласно СанПиН 2.2.2/2.4.1340-03 должны быть обеспечены оптимальные параметры микроклимата для работ категории 1а.

Нормативные требования к показателям микроклимата рабочих мест производственных помещений приведены в СанПиН 2.2.4.3359-16 «Санитарно-эпидемиологические требования к физическим факторам на рабочих местах» .

Оптимальные величины параметров микроклимата для категории работ 1а приведены в таблице 7.

В соответствии с СанПиНом 2.2.2/2.4.1340-03, в помещениях, оборудованных ПЭВМ, должна проводиться ежедневная влажная уборка, а также проветривание после каждого часа работы на ПЭВМ.

Таблица 8 - Оптимальные величины параметров микроклимата

Период года	Категория работ по уровням энергозатрат, Вт	Температура воздуха, °С	Температура поверхностей, °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

4.7. Требования к электробезопасности

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

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

Для 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.

Согласно документу «Правила устройства электроустановок» (ПУЭ) электробезопасность работающих обеспечивается конструкцией электроустановок; техническими способностями и средствами защиты, организационными средствами защиты. Предусмотрены следующие технические способы и средства защиты от поражения электрическим током:

1. Обеспечение недоступности токоведущих частей, находящихся под напряжением для случайного прикосновения;

2. Устранение опасности поражения при появлении напряжения на нетоковедущих частях электрооборудования посредством заземления (зануления).

4.8. Пожарная безопасность

Постановление Правительства РФ от 25.04.2012 N 390 (ред. от 21.03.2017) "О противопожарном режиме" устанавливают следующие правила:

1. В отношении каждого объекта (за исключением индивидуальных жилых домов) руководителем (иным уполномоченным должностным лицом) организации (индивидуальным предпринимателем), в пользовании которой на праве собственности или на ином законном основании находятся объекты (далее - руководитель организации), утверждается инструкция о мерах пожарной безопасности в соответствии с требованиями;
2. Лица допускаются к работе на объекте только после прохождения обучения мерам пожарной безопасности;
3. Лица допускаются к работе на объекте только после прохождения обучения мерам пожарной безопасности;
4. Обучение лиц мерам пожарной безопасности осуществляется путем проведения противопожарного инструктажа и прохождения пожарно-технического минимума;
5. 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;
6. Руководитель организации назначает лицо, ответственное за пожарную безопасность, которое обеспечивает соблюдение требований пожарной безопасности на объекте;
7. В складских, производственных, административных и общественных помещениях, местах открытого хранения веществ и материалов, а также размещения технологических установок руководитель организации обеспечивает наличие табличек с номером телефона для вызова пожарной охраны;
8. На объекте с массовым пребыванием людей (кроме жилых домов), а также на объекте с рабочими местами на этаже для 10 и более человек руководитель организации обеспечивает наличие планов эвакуации людей при пожаре;
9. 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;
10. Хранение огнетушителя осуществляется в соответствии с требованиями инструкции по его эксплуатации;
11. Запрещается на территориях, прилегающих к объектам, в том числе к жилым домам, а также к объектам садоводческих, огороднических и дачных некоммерческих объединений граждан, оставлять емкости с легковоспламеняющимися и горючими жидкостями, горючими газами;

12. Руководитель организации обеспечивает наличие на дверях помещений производственного и складского назначения и наружных установках обозначение их категорий по взрывопожарной и пожарной опасности;

13. Руководитель организации обеспечивает устранение повреждений толстослойных напыляемых составов, огнезащитных обмазок, штукатурки, облицовки плитными, листовыми и другими огнезащитными материалами, в том числе на каркасе, комбинации этих материалов, в том числе с тонкослойными вспучивающимися покрытиями строительных конструкций, горючих отделочных и теплоизоляционных материалов, воздуховодов, металлических опор оборудования и эстакад, а также осуществляет проверку состояния огнезащитной обработки (пропитки) в соответствии с инструкцией завода-изготовителя с составлением протокола проверки состояния огнезащитной обработки (пропитки). Проверка состояния огнезащитной обработки (пропитки) при отсутствии в инструкции сроков периодичности проводится не реже 1 раза в год;

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

15. На объектах запрещается:

15.1. Хранить и применять на чердаках, в подвалах и цокольных этажах легковоспламеняющиеся и горючие жидкости, порох, взрывчатые вещества, пиротехнические изделия, баллоны с горючими газами, товары в аэрозольной упаковке, целлулоид и другие пожаровзрывоопасные вещества и материалы, кроме случаев, предусмотренных иными нормативными документами по пожарной безопасности;

15.2. Использовать чердаки, технические этажи, вентиляционные камеры и другие технические помещения для организации производственных участков, мастерских, а также для хранения продукции, оборудования, мебели и других предметов;

15.3. Размещать в лифтовых холлах кладовые, киоски, ларьки и другие подобные помещения;

15.4. Устраивать в подвалах и цокольных этажах мастерские, а также размещать иные хозяйственные помещения, размещение которых не допускается нормативными документами по пожарной безопасности, если нет самостоятельного выхода или выход из них не изолирован противопожарными преградами от общих лестничных клеток;

15.5. 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;

15.6. 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);

15.7. Загромождать мебелью, оборудованием и другими предметами двери, люки на балконах и лоджиях, переходы в смежные секции и выходы на наружные эвакуационные лестницы, демонтировать межбалконные лестницы, заваривать и загромождать люки на балконах и лоджиях квартир;

15.8. Проводить уборку помещений и стирку одежды с применением бензина, керосина и других легковоспламеняющихся и горючих жидкостей, а также производить отогревание замерзших труб паяльными лампами и другими способами с применением открытого огня;

15.9. Остеклять балконы, лоджии и галереи, ведущие к незадымляемым лестничным клеткам;

15.10. Устраивать в лестничных клетках и поэтажных коридорах кладовые и другие подсобные помещения, а также хранить под лестничными маршами и на лестничных площадках вещи, мебель и другие горючие материалы;

15.11. Устраивать в производственных и складских помещениях зданий (кроме зданий V степени огнестойкости) антресоли, конторки и другие встроенные помещения из горючих материалов и листового металла;

15.12. Устанавливать в лестничных клетках внешние блоки кондиционеров;

15.13. Загромождать и закрывать проходы к местам крепления спасательных устройств;

16. Руководитель организации обеспечивает содержание наружных пожарных лестниц и ограждений на крышах (покрытиях) 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;

17. Приямки у оконных проемов подвальных и цокольных этажей зданий (сооружений) должны быть очищены от мусора и посторонних предметов;

18. Руководитель организации обеспечивает сбор использованных обтирочных материалов в контейнеры из негорючего материала с закрывающейся крышкой и удаление по окончании рабочей смены содержимого указанных контейнеров.

19. В зданиях с витражами высотой более одного этажа не допускается нарушение конструкций дымонепроницаемых негорючих диафрагм, установленных в витражах на уровне каждого этажа.

20. Руководителем организации, на объекте которой возник пожар, обеспечивается доступ пожарным подразделениям в закрытые помещения для целей локализации и тушения пожара.

21. Руководитель организации при расстановке в помещениях технологического, выставочного и другого оборудования обеспечивает наличие проходов к путям эвакуации и эвакуационным выходам.

22. Запрещается оставлять по окончании рабочего времени не обесточенными электроустановки и бытовые электроприборы в помещениях, в которых отсутствует дежурный персонал, за исключением дежурного освещения, систем противопожарной защиты, а также других электроустановок и электротехнических приборов, если это обусловлено их функциональным назначением и (или) предусмотрено требованиями инструкции по эксплуатации.

23. Запрещается:

23.1. эксплуатировать электропровода и кабели с видимыми нарушениями изоляции;

23.2. пользоваться розетками, рубильниками, другими электроустановочными изделиями с повреждениями;

23.3. обертывать электролампы и светильники бумагой, тканью и другими горючими материалами, а также эксплуатировать светильники со снятыми колпаками (рассеивателями), предусмотренными конструкцией светильника;

23.4. пользоваться электроутюгами, электроплитками, электрочайниками и другими электронагревательными приборами, не имеющими устройств тепловой защиты, а также при отсутствии или неисправности терморегуляторов, предусмотренных конструкцией;

23.5. применять нестандартные (самодельные) электронагревательные приборы;

23.6. оставлять без присмотра включенными в электрическую сеть электронагревательные приборы, а также другие бытовые электроприборы, в том числе находящиеся в режиме ожидания, за исключением электроприборов, которые могут и (или) должны находиться в круглосуточном режиме работы в соответствии с инструкцией завода-изготовителя;

23.7. размещать (складировать) в электрощитовых (у электрощитов), у электродвигателей и пусковой аппаратуры горючие (в том числе легковоспламеняющиеся) вещества и материалы;

23.8. при проведении аварийных и других строительно-монтажных и реставрационных работ использовать временную электропроводку, включая удлинители, сетевые фильтры, не предназначенные по своим характеристикам для питания применяемых электроприборов.

24. Руководитель организации обеспечивает исправное состояние знаков пожарной безопасности, в том числе обозначающих пути эвакуации и эвакуационные выходы;

25. Запрещается пользоваться неисправными газовыми приборами, а также устанавливать (размещать) мебель и другие горючие предметы и материалы на расстоянии менее 0,2 метра от бытовых газовых приборов по горизонтали и менее 0,7 метра - по вертикали (при нависании указанных предметов и материалов над бытовыми газовыми приборами);

26. В соответствии с инструкцией завода-изготовителя руководитель организации обеспечивает проверку огнезадерживающих устройств (заслонок, шиберов, клапанов и др.) в воздуховодах, устройств блокировки вентиляционных систем с автоматическими установками пожарной сигнализации или пожаротушения, автоматических устройств отключения вентиляции при пожаре;

27. При эксплуатации систем вентиляции и кондиционирования воздуха запрещается:

27.1. оставлять двери вентиляционных камер открытыми;

27.2. закрывать вытяжные каналы, отверстия и решетки;

27.3. подключать к воздуховодам газовые отопительные приборы

27.4. выжигать скопившиеся в воздуховодах жировые отложения, пыль и другие горючие вещества;

28. Руководитель организации определяет порядок и сроки проведения работ по очистке вентиляционных камер, циклонов, фильтров и воздуховодов от горючих отходов с составлением соответствующего акта, при этом такие работы проводятся не реже 1 раза в год;

29. Руководитель организации обеспечивает укомплектованность пожарных кранов внутреннего противопожарного водопровода пожарными рукавами, ручными пожарными стволами и вентилями, организует перекатку пожарных рукавов (не реже 1 раза в год);

30. Руководитель организации обеспечивает исправное состояние систем и средств противопожарной защиты объекта (автоматических (автономных) установок пожаротушения, автоматических установок пожарной сигнализации , установок систем противодымной защиты, системы оповещения людей о пожаре, средств пожарной сигнализации, противопожарных дверей, противопожарных и дымовых клапанов, защитных устройств в противопожарных преградах) и организует не реже 1 раза в квартал проведение проверки работоспособности указанных систем и средств противопожарной защиты объекта с оформлением соответствующего акта проверки.

31. Выбор типа и расчет необходимого количества огнетушителей следует производить в зависимости от огнетушащей способности, предельной площади, класса пожара горючих веществ и материалов защищаемом помещении или на объекте согласно СП 9.13130.2009.

Для помещений Таможенного управления актуальны следующие классы пожаров:

Класс А - пожары твердых веществ, основном органического происхождения, горение которых сопровождается тлением (древесина, текстиль, бумага).

Класс Е - пожары, связанные с горением электроустановок.

Для данных классов пожаров, исходя из рекомендация СП 9.13130.2009, следует применять порошковые огнетушители.

Огнетушители следует располагать на защищаемом объекте в соответствии с требованиями ГОСТ 12.4.009 таким образом, чтобы они были защищены от воздействия прямых солнечных лучей, тепловых потоков, механических воздействий и других неблагоприятных факторов (вибрация, агрессивная среда,

повышенная влажность и т.д.). Они должны быть хорошо видны и легкодоступны в случае пожара. Предпочтительно размещать огнетушители вблизи мест наиболее вероятного возникновения пожара, вдоль путей прохода, а также около выхода из помещения. Огнетушители не должны препятствовать эвакуации людей во время пожара.

Огнетушители, введенные в эксплуатацию, должны подвергаться техническому обслуживанию, которое обеспечивает поддержание огнетушителей в постоянной готовности к использованию и надежную работу всех узлов огнетушителя в течение всего срока эксплуатации. Техническое обслуживание включает в себя периодические проверки, осмотры, ремонт, испытания и перезарядку огнетушителей.

4.8. Сравнение параметров рабочего места с допустимыми нормами.

Для того чтобы определить соответствие условий труда требованиям нормативных документов необходимо провести сравнительный анализ требований, установленных к рабочим местам, оборудованным ПЭВМ и фактических параметров рабочего места. Схема размещения рабочего места приведена на Рисунке 1. Площадь помещения 28м^2, оконный проем, шириной 1,8м размещается слева. В помещении присутствует естественное и искусственное освещение.

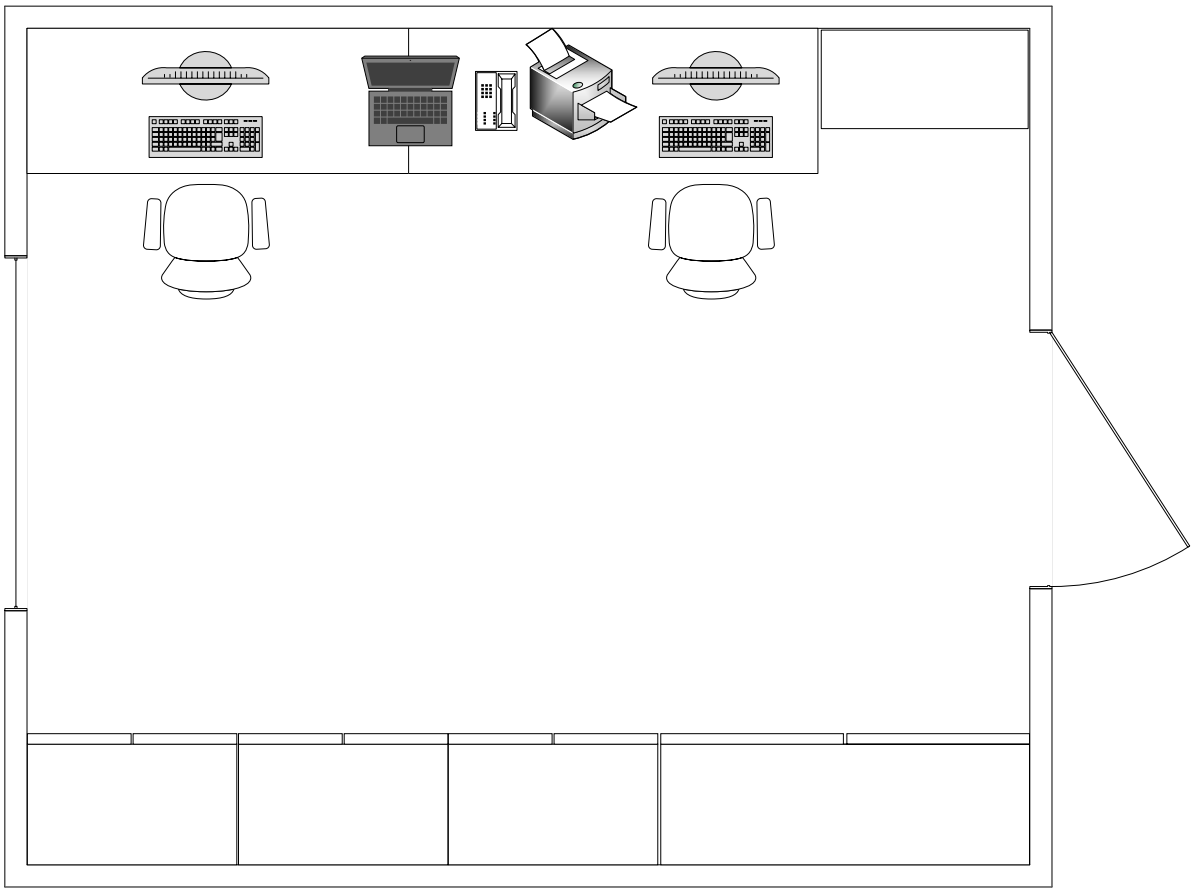


Рисунок 1 – схема помещения Таможенного управления

Перечень нормируемых параметров для рабочего места, сравнение их допустимых нормы и фактические значений на рабочем месте представлены в таблице 9.

Таблица 9– Сравнение параметров рабочего места с допустимыми нормами.

Нормируемые параметры	Допустимые нормы	Фактические значения
Высота рабочей поверхности стола	от 680 до 800мм, либо 725мм	780мм
Модульные размеры рабочей поверхности стола	Ширина 800, 1000, 1200, 1400мм, глубина 800 и 1000мм	Ширина 1400мм глубина 800 мм
Ширина и глубина поверхности сиденья	Не менее 400мм	Ширина 500мм Глубина 450мм
Подставка для ног	Присутствует	Отсутствует
Регулировка высоты сидения	400 - 550 мм	400 - 550 мм
Площадь на одно рабочее место	не менее 4,5м2	14м2
Падение естественного света	Преимущественно слева	Слева
Освещенность поверхности стола	300-500 лк	334 лк
Уровень звука	80 дБА	21 дБА
Параметры микроклимата (кат. 1а)	Температура воздуха 22-24° С Влажность воздуха 40-60%	Температура 21° С Влажность воздуха 45%

На основе проведенного анализа было установлено, что условия труда на рабочем месте не полностью соответствуют требованиям безопасности. Необходимо дополнение рабочего места подставкой для ног.

4.9. Вывод по четвертой главе

В рамках данной главы был произведен анализ типового рабочего места таможенного управления на соответствие санитарным правилам. Были рассмотрены общие требования к организации рабочих мест пользователей, обозначены требования к:

- помещениям для размещения рабочего места;
- уровням шума на рабочих местах;
- освещению на рабочих местах;
- микроклимату;
- электробезопасности;

Установлены основные требования РФ к пожарной безопасности объекта.

На основе полученных данных были формализованы санитарные требования рабочего места. Произведен замер всех необходимых параметров типового рабочего места сотрудника Таможенного управления. Дальнейшее сравнение выявленных результатов с требованиями показало, что рабочее место полностью соответствует санитарным правилам и не требует изменения

ЗАКЛЮЧЕНИЕ

Результатом выпускной квалификационной работы является модернизация действующей защиты информации персональных данных в Таможенном управлении. В результате работы был проведен предварительный анализ соответствия текущего уровня защиты объекта информатизации ИСПДн «ОПСУР» Таможенного управления требованиям законодательства в сфере защиты информации, а именно:

– требованиям, предусмотренным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

– требованиям по обеспечения уровня защищенности персональных данных, утвержденных постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– требованиям, утвержденных приказом 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».

По полученным данным были произведен анализ угроз и выявлены актуальные, составлена модель угроз (Приложение Б) и модель нарушителя, произведена актуализация технических средств вычислительной техники, их окружения, расположения и линий коммуникаций. Для оценки актуальность угрозы утечки информации по каналам побочных электромагнитных излучений и наводок(ПЭМИН) произведен замер расстояния, на которое распространяется информативный сигнал от всех ОТСС. На основании замеров был составлен протокол оценки защищенности объекта информатизации информационной системы персональных данных «ОПСУР» Таможенного управления на соответствие требованиям по защите информации от утечки по каналам ПЭМИН (Приложение А).

В результате полученных данных были выявлены основные направления модернизации текущей системы защиты.

Для нейтрализации угроз НСД предлагается установка и настройка СЗИ от НСД Dallas Lock 8.0-C.

Антивирусная защита остается без изменений и обеспечивается средствами сертифицированного ПО Kaspersky Endpoint Security 10 для Windows.

Для устранения выявленных недостатков по части организационно-распорядительной документации, её дополнили следующими документами:

1. инструкция лица, ответственного за организацию обработки персональных данных в Таможенном управлении (Приложение Г);

2. перечень должностей служащих и работников Таможенного управления, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;

3. перечень лиц, допущенных к обработке персональных данных в ИСПДн «ОПСУР» Таможенного управления;

4. инструкция по организации учета, использования и уничтожения носителей персональных данных в Таможенном управлении (Приложение Д);

На основании обновленных сведений также был составлен технический паспорт (Приложение Е).

Правильная организация рабочего пространства сотрудника является залогом его успешной и продолжительной службы. Наиболее продолжительный аспект работы в Таможенном управлении связан с взаимодействием с информационной системой посредствам вычислительной техники, по этой причине важно обеспечить соответствие рабочих мест сотрудников действующим нормам стандартов по безопасности жизнедеятельности. Реализация требований санитарных правил позволит предотвратить неблагоприятное влияния на здоровье человека вредных факторов производственной среды и трудового процесса при работе с ПЭВМ.

Был произведен анализ типового рабочего места таможенного управления на соответствие санитарным правилам. Были рассмотрены общие требования к организации рабочих мест пользователей, обозначены требования к:

- помещениям для размещения рабочего места;
- уровням шума на рабочих местах;
- освещению на рабочих местах;
- микроклимату;
- электробезопасности;

Установлены основные требования РФ к пожарной безопасности объекта.

На основе полученных данных были формализованы санитарные требования рабочего места. Произведен замер всех необходимых параметров типового рабочего места сотрудника Таможенного управления. Дальнейшее сравнение выявленных результатов с требованиями показало, что рабочее место не полностью соответствует санитарным правилам и требует изменения. Необходимо дополнение рабочего места подставкой для ног.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. «Об информации, информационных технологиях и защите информации»: Федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ: (ред. От 01.01.2017) // КонсультантПлюс. Технология 3000: Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2015.

2. «О персональных данных»: Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ: (ред. от 01.03.2017) // КонсультантПлюс. Технология 3000: Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2015.

3. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»: приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 23.03.2017):// КонсультантПлюс. Технология 3000: Версия Проф [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2015.

4. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (Выписка): утверждена ФСТЭК РФ от 15.02.2008:// КонсультантПлюс. Технология 3000: Версия Проф [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2015.

5. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»: утверждена ФСТЭК РФ 14.02.2008:// КонсультантПлюс. Технология 3000: Версия Проф [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2015.

6. ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения». – М.: Стандартинформ, 2009. – 16 с.

7. ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования». – М.:Стандартинформ,2000. – 11 с.

8. Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения». – Гостехкомиссия России. М.: Военное издательство, 1992. – 7 с.

9. ГОСТ Р 50.1.056-2005 «Техническая защита информации. Основные термины и определения». – М.: Стандартинформ, 2006. — 15 с.

10. ГОСТ Р 50922 – 2006 «Защита информации. Термины и определения». – М.: Стандартинформ, 2008. – 11 с..

11. Р 50.1.056-2005 «Техническая защита информации. Основные термины и определения». – М.: Стандартинформ, 2006. – 12 с.

12. ГОСТ 12.4.009-83. Межгосударственный стандарт. Система стандартов безопасности труда. Пожарная техника для защиты объектов. Основные виды. Размещение и обслуживание // КонсультантПлюс [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=ESU&n=9134#0

13. СанПиН 2.2.4.3359-16. Санитарно-эпидемиологические требования к физическим факторам на рабочих местах // Информационная система МЕГАНОРМ [Электронный ресурс]. – Режим доступа: http://meganorm.ru/Index2/1/4293753
/4293753139.htm

14. СанПиН 2.2.2/2.4.1340-03. Гигиенические требования к персональным электронно-вычислительным машинам и организации работы — М.: Изд-во стандартов, 2003. — 32 с.

15. "Трудовой кодекс Российской Федерации" от 30.12.2001 N 197-ФЗ (ред. от 03.07.2016) (с изм. и доп., вступ. в силу с 01.01.2017) // КонсультантПлюс [Электронный ресурс]. – http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=201079&fld=134&dst=1000000001,0&rnd=0.7021406734602476#0

ПРИЛОЖЕНИЕ А

Директор
ООО «ЦЗИ «Эгида»
_____ Кулдыбаева И.У.

«____» _____ 2017 г.

ПРОТОКОЛ

аттестационных испытаний объекта информатизации

Информационной системы персональных данных «ОПСУР» Таможенного управления на соответствие требованиям по защите информации от утечки по каналам ПЭМИН

1 ОБЩИЕ ПОЛОЖЕНИЯ

Аттестационная комиссия ООО ЦЗИ «Эгида», Лицензия ФСТЭК России № 2712 от 30.09.2015 г. в составе Кулдыбаевой И.У., Дьяконова А.Н. провела оценку защищенности объекта информатизации – информационной системы персональных данных «ОПСУР» Таможенного управления (далее АС), на соответствие требованиям по защите информации от утечки по каналам ПЭМИН.

Заявитель аттестационных испытаний объекта информатизации – Таможенное управление.

Объект информатизации принадлежит Заявителю.

Заявленный класс АС – 1Г – многопользовательская с разными правами доступа к информации.

Состав основных технических средств и систем (ОТСС) объекта информатизации приведен в таблице 1.

Состав системного и прикладного программного обеспечения, а также средств и систем защиты информации объекта информатизации приведен в Техническом паспорте.

Таблица 10

№ п/п	Тип ОТСС	Заводской номер	Сведения по сертификации, специсследованиям и спецпроверкам
1	ПЭВМ №1, СПЗ № 1		
1.1	Системный блок HP	1013400958	-
1.2	Монитор Samsung SyncMaster 943B	1013400350	
1.3	Клавиатура HP	721720-251	-
1.4	Манипулятор «мышь» HP	672652-001	-
1.5	Принтер HP LaserJet 5000	1360678	-
1.6	Считыватель Athena IIIe	110605-067901016	-
1.7	ИБП Powerman Brick 600	571VFW11-02	-
2	ПЭВМ №2, СПЗ № 2		
2.1	Системный блок Helios Profice VLX-310	1040200455	-
2.2	Монитор Samsung SyncMaster 943B	1040200455	-

№ п/п	Тип ОТСС	Заводской номер	Сведения по сертификации, специсследованиям и спецпроверкам
2.3	Клавиатура Defender HB-520	11647-140827-07361	-
2.4	Манипулятор «мышь» Defender DF2330B	68060115019	-
2.5	МФУ HP Laser Jet 1018	1040200129	-
2.6	Считыватель Athena IIIe	110605-067901016	-
2.7	ИБП Ippon smart power PRO 1000	FDF2302	-
3	ПЭВМ №3, СПЗ № 3		
3.1	Системный блок	10134000317	-
3.2	Монитор AOC e205Sda	10134000317	-
3.3	Клавиатура Genius GK-100011	XP11BSB10883	-
3.4	Манипулятор «мышь» Logitech B110	810-001317	-
3.5	Считыватель Athena IIIe	110605-067901016	-
3.6	ИБП Powerman Brick 600	571VFW11-02	
4	ПЭВМ №4, СПЗ № 4		
4.1	Системный блок KraftWay	10549869	-
4.2	Монитор Samsung SyncMaster 943B	1040200491	-
4.3	Клавиатура KraftWay	6L83400789B	-
4.4	Манипулятор «мышь» A4tech Q3-350	-	-
4.5	Принтер Lexmor KMX611de	70167PHHOBRW6	-
4.6	Считыватель Athena IIIe	110605-067901016	-
4.7	ИБП Ippon smart power PRO 400	GFDR23T	-
5	ПЭВМ №5, Кабинет № 323		

№ п/п	Тип ОТСС	Заводской номер	Сведения по сертификации, специсследованиям и спецпроверкам
5.1	Системный блок «НПП Системные ресурсы»	1013400100	-
5.2	Монитор Samsung SyncMaster 1940B	1013400100	-
5.3	Клавиатура Logitech	820-003902	-
5.4	Манипулятор «мышь» Logitech RX250	810-003902	-
5.5	Считыватель Athena IIIe	110605-067901016	-
5.6	ИБП APC Back-ups 650va	1086-34FGH-001	-
6	ПЭВМ №6, Кабинет № 313		
6.1	Системный блок Helios Profice VLX-310	1013400097	-
6.2	Монитор Samsung SyncMaster 1940B	1013400097	-
6.3	Клавиатура BTC	8711952	-
6.4	Манипулятор «мышь» Logitech RX-250	810-000208	-
6.5	Принтер HP LaserJet 1018	VNC3L77452	-
6.6	Считыватель Athena IIIe	110605-067901016	-
6.7	ИБП Ippon smart power PRO 400	QPTM284W	-

2 ПОСЛЕДОВАТЕЛЬНОСТЬ ПРОВЕДЕНИЯ ИСПЫТАНИЙ

2.1 Аттестационные испытания объекта информатизации проводились в соответствии в следующем порядке:

– определение состава использованных для обработки информатизации технических средств, их комплектность и соответствие данным, указанным в эксплуатационной документации;

– проверка выполнение требований от утечки за счет побочных электромагнитных излучений (ПЭМИ);

– проверка выполнения требований от утечки за счет наводок на вспомогательные технические средства и системы (ВТСС);

– проверка выполнения требований от утечки информативного сигнала по цепям электропитания и заземления;

– комплексные испытания объекта, в т.ч. при возникновении внештатных ситуаций.

2.2 Испытания проводились в следующей последовательности:

– ознакомление и экспертная оценка протоколов по результатам стендовых и объектовых специальных исследований, и заключений по специальным проверкам на предмет соответствия их оформления требованиям нормативно-методическим документов, полноты и правильности расчетов;

– ознакомление с технической документацией на ОТСС, ВТСС, систему электропитания и заземления;

– ознакомление с эксплуатационной документацией;

– экспертиза предоставленной технической и эксплуатационной документации на соответствие требованиям нормативно-технических документов;

– проведение аппаратурных (инструментальных) замеров физических параметров информативного сигнала, сравнение полученных результатов с результатами, указанными в предоставленных документах;

– выводы по каждому разделу.

2.3 При проведении оценки защищенности использовались следующие нормативные и методические документы:

– ГОСТ Р 50752-95. Информационная технология. Защита информации от утечки за счет побочных электромагнитных излучений при ее обработке средствами вычислительной техники. Методы испытаний;

– ГОСТ Р 29339-92. Информационная технология. Защита информации от утечки за счет побочных электромагнитных излучений при ее обработке средствами вычислительной техники. Общие технические требования;

– Специальными требованиями и рекомендациями по технической защите конфиденциальной информации, Гостехкомиссия России, утвержден приказом от 30 августа 2002 г.

– Сборником временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам, Гостехкомиссия России, 2002 г.

2.4 Измерения проводились по электрической и магнитной составляющим электромагнитного поля с применением средств измерений, приведенных в таблице 2.

Таблица 2

Тип	Наименования средств измерений и вспомогательного оборудования	Заводской номер	Диапазон частот	Дата очередной поверки
Средства измерений				
Анализатор спектра	Rohde & Schwarz FS300	103032	9-3000 МГц	14.05.2018
Комплект антенн измерительных «Альбатрос-2»	АГМ-30 АГ-50 АГ-1000 АГ-2000	А189.1 А189.2 А189.3 А189.4	0,009-2000МГц	23.04.2018
Универсальный генератор сигналов	RIGOL DG5352	DG5C122200035	1мкГц – 350 МГц	-
Пробник напряжения	«Шмель»	08.323	0,009-300МГц	22.04.2018

В качестве тест-сигналов использовались сигналы, создаваемые специализированными тестирующими программами (сборник тестовых программ ЗАО «ЦБИ-сервис»).

3 РЕЗУЛЬТАТЫ ИСПЫТАНИЙ ПО КАНАЛУ ПЭМИН

3.1 Определение состава использованных для обработки информатизации технических средств, их комплектность и соответствие данным, указанным в эксплуатационной документации

Проведена проверка состава технических средств, предназначенных для обработки конфиденциальной информации на соответствие представленной документации.

Выводы: *Состав используемых для обработки конфиденциальной информации технических средств соответствует данным, представленным в документации.*

3.2 Проверка выполнения требований от утечки за счет ПЭМИ от ОТСС

Для определения значений зоны R2 использовался метод, изложенный во «Временной методике оценки защищенности ОТСС, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации».

Результаты измерений частот и уровней напряженности поля составляющих тест-сигналов от ПЭВМ, проведенных на расстоянии 1 метр от нее в направлениях минимального расстояния до границы контролируемой зоны и максимального излучения приведены в Таблице 3.

Таблица 3

F, МГц	E_0, дБ	H_0, дБ	$E_Ш$, дБ	$H_Ш$, дБ	E_c, мкВ/м	H_c, дБ	R_i, м
1. ПЭВМ №1, СПЗ №1, Режим работы монитора – 1920 на 1080 точек область экрана, частота обновления 60 Гц,							
Уровень информативного сигнала не превышает уровня помех							
3. ПЭВМ №2, СПЗ №2, Режим работы монитора – 1920х1080 точек область экрана, частота обновления 60 Гц							
74.30	56.44	-	44.53	-	642.00	-	2.52
222.8	39.97	-	33.51	-	87.67	-	1.76
371.3	52.83	-	41.91	-	419.93	-	2.37
3. ПЭВМ №3, СПЗ №3, Режим работы монитора – 1920х1080 точек область экрана, частота обновления 60 Гц							
Уровень информативного сигнала не превышает уровня помех							
4. ПЭВМ №4, СПЗ №4, Режим работы монитора – 1440х900 точек область экрана, частота обновления 60 Гц							
159.60	59.11	-	40.95	-	895.68	-	3.66
5. ПЭВМ №5, СПЗ №5,, Режим работы монитора – 1920х1080 точек область экрана, частота обновления 60 Гц							

Уровень информативного сигнала не превышает уровня помех							
6. ПЭВМ №6, СПЗ №6, Режим работы монитора – 1280x1024 точек область экрана, частота обновления 60 Гц							
54.0	53.35	-	49.92	-	343.65	-	1.35
162.0	56.91		43.22		685.50		2.81

Примечание.

E_0 (H_0), $E_Ш$ ($H_Ш$), дБ – измеренные уровни напряженности электромагнитного поля по электрической (магнитной) составляющей при работе ОТСС в тестируемом режиме и при выключенном ОТСС соответственно;

E_c (H_c), дБ – рассчитанные уровни напряженности электромагнитного поля по электрической (магнитной) составляющей, создаваемые информативным сигналом. Величины E_0 , $E_Ш$ и E_c в дБ связаны между собой соотношением:

$$E_c = 20 \cdot \lg \sqrt{10^{E_0/10} - 10^{E_ш/10}}$$

Измерения по электрической и магнитной составляющим электромагнитного поля проводились относительно 1 мкВ/м и 1 мкА/м, в полосе частот 0.2 кГц для диапазона 9 - 150 кГц, 9 кГц – для диапазона 0.15 – 30 МГц и 100 кГц для диапазона свыше 30 МГц.

Магнитная составляющая ПЭМИ не выявлена.

Для следующих режимов обработки информации уровень тест-сигнала на границе контролируемой зоны ниже уровня естественных помех:

- набор текста с клавиатуры;
- запись – считывание информации на ЖМД;
- запись – считывание информации на CD/DVD-привод;
- обмен информацией с принтером;
- вывод информации на печать.

Радиоизлучений, модулированных информативным сигналом из-за паразитной генерации в узлах (элементах) ПЭВМ, не выявлено.

Выводы: Защищенность ОТСС от утечки конфиденциальной информации по каналу ПЭМИ обеспечивается, так как рассчитанный требуемый радиус КЗ меньше минимального расстояния от ОТСС до ее границы. Дополнительных средств защиты не требуется.

3.3 Проверка выполнения требований от утечки за счет наводок информативного сигнала на цепь электропитания, трубопровод системы отопления

Измерениям подвергался информативный сигнал, наведенный от АС на линии, приведенные в таблице 4, расположенные совместно с АС и имеющие выход за пределы контролируемой зоны объекта. Комплектация ОТСС указана в таблице 1.

Таблица 4

№ пп	Линии (коммуникации)	Минимальная протяженность до границы КЗ, м.
1	Линия системы отопления	2
2	Линия телефонной связи	3
3	Линия электропитания	5
4	Линия пожарной сигнализации	4
5	Линия охранной сигнализации	2
6	Линия локальной вычислительной сети	3

При проведении измерения руководствовались следующими нормативными документами:

- «Временная методика оценки защищенности конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счет наводок на вспомогательные технические средства и системы и их коммуникации». Гостехкомиссия России. М., 2002.

Информативный сигнал измерялся на частотах обнаруженных информативных ПЭМИ в диапазоне 0,1…250 МГц путем подключения пробника напряжения, соединенного с входом анализатора спектра.

Результаты измерений наведенного информативного сигнала и расчета значения допустимого пробега линий (коммуникаций) до границы КЗ представлены в таблице 5.

Таблица 5

F_i, МГц	$U_{(с+ш)i}$, дБ	$U_{ші}$, дБ	$U_{сі}$, дБ	$U_{1измі}$, мкВ	$U_{2измі}$, мкВ	$K_{пі}$, дБ	R_i, м	$R_{КЗ}$, м
ПЭВМ №1 - ПЭВМ №6								
Линия системы отопления								
Уровень информативного сигнала не превышает уровня помех								
Линия телефонной связи								
Уровень информативного сигнала не превышает уровня помех								
Линия электропитания								
Уровень информативного сигнала не превышает уровня помех								
Линия пожарной сигнализации								
Уровень информативного сигнала не превышает уровня помех								
Линия охранной сигнализации								
Уровень информативного сигнала не превышает уровня помех								
Линия локальной вычислительной сети								
Уровень информативного сигнала не превышает уровня помех								

Измерения производились в полосе частот 9 кГц для диапазона до 30 МГц и 120 кГц для диапазона свыше 30 МГц.

Выводы: *защищенность информации, обрабатываемой ОТСС, от ее утечки за счет наводок информативного сигнала обеспечивается. Дополнительные меры защиты не требуются.*

4 ВЫВОДЫ АТТЕСТАЦИОННОЙ КОМИССИИ

По результатам аттестационных испытаний комиссия считает, что применяемые организационно-технические средства и меры защиты ***соответствуют*** *требуемому уровню защищенности информации от утечки за счет ПЭМИН.*

Члены комиссии

_____И.У. Кулдбыаева

_____А.Н. Дьяконов

ПРИЛОЖЕНИЕ Б

СОГЛАСОВАНО
Директор
ООО «ЦЗИ «Эгида»
_____ Кулдыбаева И.У.

«____» _____ 2017 г.

УТВЕРЖДАЮ
Начальник Таможенного управления

_____

«____» _____ 2017 г.

МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
При ее обработке в информационной системе персональных данных «ОПСУР»
Таможенного управления

1. Общие положения

Данная модель угроз безопасности информации при ее обработке в информационной системе персональных данных «ОПСУР» (далее – ИСПДн) Таможенного управления разработана на основании:

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

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

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

4) банка данных угроз безопасности информации (bdu.fstec.ru).

Угрозы безопасности персональных данных (далее – информации), обрабатываемых в ИС, содержащиеся в настоящей Модели угроз, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств реализации угроз безопасности в ИС. Модель угроз может быть пересмотрена по решению Начальника Таможенного управления на основе периодически проводимого анализа и оценки угроз безопасности информации с учетом особенностей и (или) изменений ИС, а также по результатам мероприятий по контролю выполнения требований к обеспечению безопасности информации при ее обработке в ИС.

2. Описание ИС

ИСПДн «ОПСУР» предназначена для анализа и контроля совершения таможенных операций в отношении перемещаемых через таможенную границу РФ товаров и транспортных средств международной перевозки, в том числе в целях выявления и предотвращения случаев нарушения требований таможенного законодательства.

В ИС осуществляется обработка персональных данных менее чем 100 000 субъектов ПДн. Субъектами ПДн являются граждане РФ, обратившиеся со своей в Таможенное управление с целью совершения таможенных операций по перемещению через таможенную границу РФ товаров и транспортных средств международной перевозки.

Общие данные об ИС:

Наименование ИС	Информационная система персональных данных «ОПСУР»
Оператор	Таможенное управление
Пользователи ИС	Работники отдела применения системы управления рисками,
Тип ИС	Информационная система, обрабатывающая иные категории персональных данных субъектов персональных данных, являющихся и не являющихся работниками оператора

Объем обрабатываемых персональных данных	Менее 100 000
Структура информационной системы	ИС представляет собой шесть автоматизированных рабочих мест (далее – АРМ), соединенных в локальную сеть.
Подключение информационной системы к сетям общего пользования и (или) сетям международного информационного обмена	Имеет подключение к ведомственной сети – скоростной информационной магистрали Таможенных органов
Режим обработки персональных данных	Многопользовательская система
Режим разграничения прав доступа пользователей	С разграничением прав доступа
Доступ в ИС	По имени пользователя (логину), паролю и аппаратному идентификатору
Взаимодействие с другими информационными системами	Имеет один канал связи с БДн в составе АИС «ЕБВР».
Характеристики безопасности персональных данных, обрабатываемых в информационной системе	Требуется обеспечение конфиденциальности, целостности и доступности персональных данных
Местонахождение технических средств информационной системы	Все технические средства находятся в пределах Российской Федерации

Возможность возникновения угроз 1-го и 2-го типа, связанных с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении (далее – ПО), используемом в автоматизированной системе исключается ввиду отсутствия мотивации осуществления деятельности, связанной с нарушением характеристик безопасности информации у нарушителей, которые могут использовать данные уязвимости (разведывательные службы, разработчики операционных систем), а также отсутствия информации в ИС, ценной для данных нарушителей. Остальные типы нарушителей, ввиду сложности и больших финансовых затрат для реализации уязвимостей не рассматриваются.

В соответствии с частью 6 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства РФ от 1 ноября 2012 г. № 1119, для ИС актуальны угрозы 3-го типа, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном ПО, используемом в информационной системе.

Основываясь на порядке определения требуемого уровня защищенности, 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», для персональных данных, обрабатываемых в ИС, необходимо обеспечить 4 (четвертый) уровень защищенности.

ИС расположена по адресу: _____

Границей контролируемой зоны являются ограждающие конструкции помещения.

Работа пользователей ИС определяется утвержденной инструкцией пользователя. Данные поступают на бумажных носителях. Сотрудник вручную вносит данные в БДн АИС «ЕБВР» путем заполнения формы в веб-приложении

Данные хранятся на сервере баз данных в центральном аппарате г. Москва. Передача осуществляется по защищенному каналу связи. Права доступа пользователей к режимам обработки файлов (ввод, корректировка, просмотр, печать) утверждаются в установленном порядке. Работа пользователя возможна только после успешного прохождения процедуры аутентификации в веб-приложении АИС «ЕБВР».

На АРМ ИС, используется антивирусная программа Kaspersky Endpoint Security 10 для Windows, а также лицензионное (или свободно распространяемое) программное обеспечение.

Резервное копирование не предусмотрено технологическим процессом. Данные на хранятся локально.

Контроль целостности компонентов операционной системы ведется СЗИ от НСД, утратившим сертификат.

Регистрация событий безопасности ИС осуществляется СЗИ от НСД, утратившим сертификат.

При определении угроз безопасности информации в ИС защите подлежат следующие объекты:

– информация, обрабатываемая в ИС;
– информационные ресурсы ИС (файлы, базы данных и т.п.);
– средства вычислительной техники, участвующие в обработке информации;
– системное и прикладное программное обеспечение;
– носители защищаемой информации, используемые в ИС в том числе носители ключевой, парольной и аутентифицирующей информации и порядок доступа к ним;
– используемые каналы (линии) связи, включая кабельные системы;
– помещение, в котором расположены компоненты ИС.

При обработке информации в ИС не используются:

– облачные технологии;
– технологии виртуализации;
– хранилища больших данных;
– суперкомпьютеры;
– грид-системы;
– мобильные устройства;
– технологии беспроводного доступа.

В связи с этим из перечня объектов угроз исключаются все объекты воздействия, связанные с неиспользуемыми при обработке информации техническими средствами и технологиями.

3. Перечень угроз, представляющих потенциальную опасность для информации, обрабатываемой в ИС

В данной модели угроз рассмотрены следующие категории угроз:
- угрозы утечки информации по техническим каналам;
- физические угрозы;
- угрозы несанкционированного доступа;
- угрозы персонала.

4. Модель вероятного нарушителя информационной безопасности

4.1 Описание возможных нарушителей

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

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

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

Внутренний нарушитель

Исходя из особенностей функционирования ИС, допущенные к ней физические лица, имеют разные полномочия на доступ к информационным, программным, аппаратным и другим ресурсам ИС в соответствии с принятой политикой информационной безопасности (правилами). К внутренним нарушителям могут относиться:
- администраторы ИС (категория I);
- пользователи ИС (категория II);
- работники, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются ресурсы ИС, но не имеющие права доступа к ресурсам (категория III);
- обслуживающий персонал (охрана, работники инженерно-технических служб и т.д.) (категория IV);
- уполномоченный персонал разработчиков ИС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИС (категория V).

На лиц I категории возложены задачи по администрированию программно-аппаратных средств ИС для интеграции и обеспечения взаимодействия различных подсистем, входящих в состав ИС. Администраторы потенциально могут реализовывать угрозы ИБ, используя возможности по непосредственному доступу к защищаемой информации, обрабатываемой и хранимой в ИС, а также к техническим и программным средствам ИС, включая средства защиты,

используемые в конкретных информационных системах, в соответствии с установленными для них административными полномочиями.

Эти лица хорошо знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и ИС в целом, а также с применяемыми принципами и концепциями безопасности. Предполагается, что они могли бы использовать стандартное оборудование либо для идентификации уязвимостей, либо для реализации угроз ИБ. Данное оборудование может быть как частью штатных средств, так и может относиться к легко получаемому (например, программное обеспечение, полученное из общедоступных внешних источников).

Кроме того, предполагается, что эти лица могли бы располагать специализированным оборудованием.

На лиц II категории возложены задачи по использованию программно-аппаратных средств и баз данных ИС. Пользователи потенциально могут реализовывать угрозы ИБ используя возможности по непосредственному доступу к защищаемой информации, обрабатываемой и хранимой в ИС, а также к техническим и программным средствам ИС, включая средства защиты, используемые в конкретных информационных системах, в соответствии с установленными для них полномочиями.

К лицам категорий I и II ввиду их исключительной роли в ИС должен применяться комплекс особых организационных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

Предполагается, что в число лиц категорий I и II будут включаться только доверенные лица и поэтому указанные лица исключаются из числа вероятных нарушителей.

Предполагается, что лица категорий III-V относятся к вероятным нарушителям.

Предполагается, что возможность сговора внутренних нарушителей маловероятна ввиду принятых организационных и контролирующих мер.

Внешний нарушитель

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

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

К внешним нарушителям могут относиться:

– бывшие работники – администраторы или пользователи ИСПД

(категория VI);

– посторонние лица, пытающиеся получить доступ к ПДн в инициативном порядке (категория VII).

Лица категории VI хорошо знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и ИС в целом, а также с применяемыми принципами и концепциями безопасности. Предполагается, что они могли бы использовать стандартное оборудование либо для идентификации уязвимостей, либо для реализации угроз ИБ. Данное оборудование может быть как частью штатных средств, так и может относиться к легко получаемому (например, программное обеспечение, полученное из общедоступных внешних источников).

Лица категории VII могут быть знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и ИС в целом, но не знакомы с применяемыми принципами и концепциями безопасности на объекте ИСПД. Предполагается, что они могли бы использовать стандартное оборудование либо для идентификации уязвимостей, либо для реализации угроз. Данное оборудование может относиться к легко получаемому (например, программное обеспечение, полученное из общедоступных внешних источников).

Лица категорий VI и VII потенциально могут реализовывать угрозы ИБ, путем физического проникновения в помещения, где расположены технические средства ИС.

Предполагается, что лица категорий VI и VII относятся к вероятным нарушителям.

4.2 Предположения об имеющейся у нарушителя информации об объектах реализации угроз

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

– информации о назначения и общих характеристиках ИС;

– информация, полученная из эксплуатационной документации;

– информация, дополняющая эксплуатационную информацию об ИС (например, сведения из проектной документации ИС).

В частности, нарушитель может иметь:

– данные об организации работы, структуре и используемых технических, программных и программно-технических средствах ИС;

– сведения об информационных ресурсах ИС: порядок и правила создания, хранения и передачи информации, структура и свойства информационных потоков;

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

– данные о реализованных в СЗИ принципах и алгоритмах;

– исходные тексты программного обеспечения ИС;

– сведения о возможных каналах реализации угроз;

– информацию о способах реализации угроз.

Предполагается, что лица категорий III - VI не владеют парольной и аутентифицирующей информацией, используемой в АИС.

Организационными мерами предполагается исключить доступ лиц категории V к техническим и программным средствам ИС в момент обработки с использованием этих средств защищаемой информации.

Предполагается полностью исключить доступ лиц категорий VI – VII к техническим и программным средствам ИС.

Степень информированности нарушителя зависит от многих факторов, включая реализованные конкретные организационные меры и компетенцию нарушителей. Поэтому объективно оценить объем знаний вероятного нарушителя в общем случае практически невозможно.

В связи с изложенным, с целью создания необходимых условий безопасности информации предполагается, что вероятные нарушители обладают всей информацией, необходимой для подготовки и реализации угроз, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты информации. К такой информации, например, относится парольная, аутентифицирующая и ключевая информация.

4.3. Предположения об имеющихся у нарушителя средствах реализации угроз

Предполагается, что нарушитель имеет:

– аппаратные компоненты системы защиты информации и ее среды функционирования;

– доступные в свободной продаже технические средства и программное обеспечение.

Предполагается что содержание и объем персональных данных, находящихся в ИС не достаточны для мотивации применения нарушителем специально разработанных технических средства и программного обеспечения.

Внутренний нарушитель может использовать штатные средства.

Состав имеющихся у нарушителя средств, которые он может использовать для реализации угроз ИБ, а также возможности по их применению зависят от многих факторов, включая реализованные на объекте ИС конкретные организационные меры, финансовые возможности и компетенцию нарушителей. Поэтому объективно оценить состав имеющихся у нарушителя средств реализации угроз в общем случае практически невозможно.

Поэтому, для определения актуальных угроз и создания СЗИ предполагается, что вероятный нарушитель имеет все необходимые для реализации угроз средства, доступные в свободной продаже, возможности которых не превосходят возможности аналогичных средств реализации угроз на информацию, содержащую сведения, составляющие государственную тайну, и технические и программные средства, обрабатывающие эту информацию.

Вместе с тем предполагается, что нарушитель не имеет:

– средств перехвата в технических каналах утечки;

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

– средств воздействия на источники и через цепи питания;

Технические и эксплуатационные характеристики ИС	Уровень защищенности		
	Высокий	Средний	Низкий
1. По территориальному размещению			
Локальная ИС, развернутая в пределах одного здания	+		
2. По наличию соединения с сетями общего пользования			
ИС, физически отделенная от сети общего пользования	+		
3. По встроенным (легальным) операциям с записями баз ПДн			
Запись, удаление, сортировка,		+	
4. По разграничению доступа к ПДн			
ИС, к которой имеет доступ определенный перечень работников организации, являющейся владельцем ИС, либо субъект ПДн		+	
5. По наличию соединений с другими базами ПДн иных ИС			
ИС, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИС	+		
6. По уровню обобщения (обезличивания) ПДн			
ИС, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)			+
7. По объему ПДн, которые предоставляются сторонним пользователям ИС без предварительной обработки			
ИС, не предоставляющая никакой информации	+		
Характеристики ИС	**57,14 %**	**28,57 %**	**14,28 %**

– средств воздействия через цепи заземления;

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

5. Определение актуальных угроз безопасности информации при обработке в ИС

5.1. Определение уровня исходной защищенности ИС

Уровень исходной защищенности ИС определен экспертным методом в соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (далее – Методика), утвержденной 14 февраля 2008 г. заместителем директора ФСТЭК России. Результаты анализа исходной защищенности приведены в Таблице 1.

Таблица 1. Уровень исходной защищенности

Таким образом, ИС имеет **средний (*Y*$_1$=5)** уровень исходной защищенности, т. к. не менее 70% характеристик ИС соответствуют уровню защищенности не ниже «средний».

5.2. Определение актуальных угроз безопасности информации

Частота реализации угроз, опасность угроз и актуальность угроз определены экспертным методом в соответствии с Методикой на основе опроса ответственных работников организации и результатов обследования ИС.

Результаты определения частоты реализации угроз, опасности угроз и актуальности угроз приведены в Таблице 2.

Продолжение приложения Б

Таблица 2. Угрозы безопасности ПДн

Угроза	Анализ реализации мер защиты	Вероятность реализации угрозы (коэффициент Y2)	Возможность реализации угрозы (коэффициент Y)	Факторы, определяющие опасность угрозы	Показатель опасности угрозы	Актуальность угрозы
Угрозы утечки информации по техническим каналам						
Угрозы утечки акустической (речевой) информации						
Угрозы утечки акустической (речевой) информации	Меры защиты не реализованы.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности защищаемой информации. Функции голосового ввода и воспроизведения ПДн акустическими средствами ИС отсутствуют.	низкая	неактуальная
Угрозы утечки видовой информации						
Угрозы утечки видовой информации	Технические средства отображения информации	низкая вероятность (2)	средняя (0,35)	Реализация угрозы может привести к нарушению	низкая	неактуальная

Продолжение приложения Б

	расположены внутри КЗ. На окнах установлены шторы и жалюзи. Работники, обрабатывающие защищаемую информацию проинструктированы о правилах работы с защищаемой информацией в присутствии посторонних.			конфиденциальности защищаемой информации. Расположение средств отображения средств вычислительной техники исключает возникновение прямой видимости между средством наблюдения и носителем защищаемой информации.		
Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок						
Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок	Мер защиты от утечки информации по каналам ПЭМИН не принято. Информативный сигнал не уходит за пределы КЗ.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации. Стоимость	низкая	неактуальная

				реализации угрозы не сопоставима с возможно полученным объемом защищаемой информации.		
Угрозы несанкционированного доступа путем физического доступа к элементам системы						
Неавторизованное проникновение внешнего нарушителя в помещение, в котором ведется обработка защищаемой информации						
Неавторизованное проникновение внешнего нарушителя в помещение, в котором ведется обработка защищаемой информации	Предпринятые меры защиты включают в себя круглосуточную охрану контролируемой зоны. В нерабочее время помещение, в котором ведется обработка защищаемой информации, закрывается на ключ и сдается под охрану. Реализован пропускной режим в здание. Ведется видеонаблюдение.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации.	средняя	неактуальная

	Регламентирован порядок доступа в помещение, где расположены технические средства ИС.					
Угрозы стихийного характера						
Угрозы, связанные с природными или техногенными катастрофами	Помещение, в котором ведется обработка защищаемой информации, оборудовано пожарной и охранной сигнализацией. Информация храниться в БД иной ИС территориально удаленной от рассматриваемой.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению целостности и доступности защищаемой информации. В связи с географическим расположением объекта, отсутствуют объективные предпосылки для осуществления угрозы.	низкая	неактуальная
Отключение электроэнергии	Технические средства оборудованы резервным источником	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению целостности и	низкая	неактуальная

Продолжение приложения Б

	бесперебойного питания.			доступности защищаемой информации. ПДн дублируются на бумажных носителях информации.		
Преднамеренные действия внешнего нарушителя						
Повреждение каналов связи (кабелей), выходящих за пределы контролируемой зоны (далее – КЗ)	Физический доступ к кабельным линиям затруднен.	маловероятно (0)	низкая (0,25)	Реализация угрозы не приведет к нарушению свойств безопасности информации.	низкая	неактуальная
Кража технических средств ИС, носителей информации	Предпринятые меры защиты включают в себя круглосуточную охрану контролируемой зоны. В нерабочее время помещение, в котором ведется обработка защищаемой информации, закрывается на	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности и доступности защищаемой информации.	средняя	неактуальная
Порча или уничтожение технических средств		маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к	средняя	неактуальная

Продолжение приложения Б

ИС, носителей информации	ключ и сдается под охрану. Реализован пропускной режим в здание. Ведется видеонаблюдение. Регламентирован порядок доступа в помещение, где расположены технические средства ИС.			нарушению целостности и доступности защищаемой информации.		
Подлог носителей, содержащих недостоверную информацию	Доступ к техническим средствам ИС ограничен кругом лиц, являющихся работниками Таможенного управления. Регламентирован порядок доступа в помещение, где расположены технические средства ИС. Защищаемая информация не хранится локально на АРМ.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению достоверности защищаемой информации.	средняя	неактуальная

Продолжение приложения Б

Кража ключей и атрибутов доступа	Предпринятые меры защиты включают в себя круглосуточную охрану контролируемой зоны. В нерабочее время помещение, в котором ведется обработка защищаемой информации, закрывается на ключ и сдается под охрану. Реализован пропускной режим в здание. Ведется видеонаблюдение. Регламентирован порядок доступа в помещение, где расположены технические средства ИС.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности защищаемой информации. Ведется учет персональных идентификаторов.	средняя	неактуальная
Кража, модификация, уничтожение информации	Предпринятые меры защиты включают в себя круглосуточную охрану контролируемой	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности и целостности	средняя	неактуальная

Продолжение приложения Б

	зоны. В нерабочее время помещение, в котором ведется обработка защищаемой информации, закрывается на ключ и сдается под охрану. Реализован пропускной режим в здание. Ведется видеонаблюдение. Регламентирован порядок доступа в помещение, где расположены технические средства ИС. Защищаемая информация не хранится локально на АРМ.			защищаемой информации.		
Несанкционированное проводное подключение к кабельной линии за пределами контролируемой зоны	ИС имеет подключение к ведомственной сети – скоростной информационной магистрали органов Таможенного управления.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой	средняя	неактуальная

Продолжение приложения Б

	Используются средства криптографической защиты информации при ее передаче.			информации.		
Внедрение аппаратных закладок в технические средства ИС	Предпринятые меры защиты включают в себя круглосуточную охрану контролируемой зоны. В нерабочее время помещение, в котором ведется обработка защищаемой информации, закрывается на ключ и сдается под охрану. Реализован пропускной режим в здание. Ведется видеонаблюдение.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации. Обслуживание технических средств осуществляется собственными силами.	средняя	неактуальная
Преднамеренные действия внутреннего нарушителя						
Кража технических средств ИС, носителей информации	Доступ к техническим средствам ИС ограничен кругом	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению	средняя	неактуальная

Продолжение приложения Б

	лиц, являющихся работниками Таможенного управления.			конфиденциальности защищаемой информации.		
Порча или уничтожение технических средств ИС, носителей информации	Информация дублируется на бумажных носителях. Регламентирован порядок доступа в помещение, где расположены технические средства ИС. Защищаемая информация не хранится локально на АРМ.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению целостности и доступности защищаемой информации.	средняя	неактуальная
Подлог носителей, содержащих недостоверную информацию	Доступ к техническим средствам ИС ограничен кругом лиц, являющихся работниками Таможенного управления. Регламентирован порядок доступа в помещение, где расположены	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению достоверности защищаемой информации. Учет носителей информации не производится.	средняя	неактуальная

Продолжение приложения Б

	технические средства ИС. Защищаемая информация не хранится локально на АРМ.					
Кража, модификация, уничтожение информации	Доступ к техническим средствам ИС ограничен кругом лиц, являющихся работниками Таможенного управления. Защищаемая информация не хранится локально на АРМ. Регламентирован порядок доступа в помещение, где расположены технические средства ИС.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности и целостности защищаемой информации. Порядок резервного копирования не регламентирован. Учет носителей информации не производится.	средняя	неактуальная
Изменение режимов работы технических средств ИС	Доступ к техническим средствам ИС ограничен кругом лиц, являющихся	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциально	средняя	неактуальная

	работниками Таможенного управления.			сти, целостности и доступности защищаемой информации. Учет носителей информации не производится.		
Повреждение каналов связи (кабелей), находящихся в пределах контролируемой зоны	Физический доступ к кабелям, находящимся в пределах контролируемой зоны затруднен. В нерабочее время помещение, в котором ведется обработка защищаемой информации, закрывается на ключ и сдается под охрану. Реализован пропускной режим в здание. Ведется видеонаблюдение.	маловероятно (0)	низкая (0,25)	Реализация угрозы не приведет к нарушению свойств безопасности информации.	низкая	неактуальная
Несанкционированное проводное подключение к кабельной линии	ИС имеет подключение к ведомственной сети – скоростной	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению	средняя	неактуальная

Продолжение приложения Б

(коммуникационному оборудованию) в пределах контролируемой зоны	информационной магистрали Таможенных органов. Нахождение посторонних лиц в помещении в отсутствие работников Таможенного управления не допускается.			конфиденциальности, целостности и доступности защищаемой информации.		
Внедрение аппаратных закладок в технические средства ИС	Доступ к техническим средствам ИС ограничен кругом лиц, являющихся работниками Таможенного управления.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации.	средняя	неактуальная
Непреднамеренные действия внутреннего нарушителя						
Непреднамеренная утрата носителей информации	Защищаемая информация не хранится локально на АРМ.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести только к нарушению конфиденциальности защищаемой информации.	средняя	неактуальная

				Учет носителей информации не производится.		
Непреднамеренный вывод из строя или изменение режимов работы технических средств ИС	Доступ к техническим средствам ИС ограничен кругом лиц, являющихся работниками Таможенного управления. Предусмотрены инструкции пользователей по работе в ИС.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению целостности и доступности защищаемой информации. Порядок резервного копирования не регламентирован.	средняя	неактуальная
Непреднамеренное повреждение каналов связи (кабелей), находящихся в пределах контролируемой зоны	Физический доступ к кабелям, находящимся в пределах контролируемой зоны затруднен.	маловероятно (0)	низкая (0,25)	Повреждение каналов связи внутри КЗ не приведет к нарушению тех. процесса обработки информации и к нарушению свойств безопасности информации.	низкая	неактуальная
Угрозы технического характера						

Продолжение приложения Б

Потеря данных в результате отказа носителей информации	Защищаемая информация не хранится локально на АРМ. ПДн дублируются на бумажных носителях информации.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению целостности и доступности защищаемой информации.	средняя	неактуальная
Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания	Обслуживание технических средств ИС осуществляется силами администратора ИС.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению целостности и доступности защищаемой информации. ПДн дублируются на бумажных носителях информации.	средняя	неактуальная
Угроза нарушения технологического/ производственного процесса из-за временных задержек, вносимых средством защиты	Обслуживание технических средств ИС осуществляется силами администратора ИС.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению доступности защищаемой информации.	средняя	неактуальная

Продолжение приложения Б

Угроза физического устаревания аппаратных компонентов	Проводится периодическое обновление технических средств.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению доступности защищаемой информации.	средняя	неактуальная
Угрозы несанкционированного доступа с применением программно-аппаратных средств (в том числе программно-математических воздействий)						
Преднамеренные действия внешнего нарушителя						
Внедрение кода или данных	Используется средство антивирусной защиты.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации.	средняя	неактуальная
Перехват вводимой и выводимой на периферийные устройства информации	Используется средство антивирусной защиты. В нерабочее время помещение, в котором ведется обработка защищаемой	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности защищаемой информации.	средняя	неактуальная

Продолжение приложения Б

	информации, закрывается на ключ и сдается под охрану. Реализован пропускной режим в здание. Ведется видеонаблюдение					
Подделка записей журнала регистрации событий	Используется СЗИ от НСД утратившее сертификат	низкая вероятность (2)	средняя (0,35)	Реализация угрозы может привести к нарушению целостности защищаемой информации.	средняя	**актуальная**
Несанкционированное изменение параметров настройки средств защиты информации	Используется СЗИ от НСД утратившее сертификат	низкая вероятность (2)	средняя (0,35)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации.	средняя	**актуальная**
Доступ к защищаемым файлам с использованием альтернативных путей доступа к ресурсам	Используется СЗИ от НСД утратившее сертификат	низкая вероятность (2)	средняя (0,35)	Реализация угрозы может привести к нарушению конфиденциальности защищаемой	средняя	**актуальная**

				информации.		
Несанкционированная модификация защищаемой информации	Используется СЗИ от НСД утратившее сертификат	низкая вероятность (2)	средняя (0,35)	Реализация угрозы может привести к нарушению целостности защищаемой информации.	средняя	**актуальная**
Несанкционированное удаление защищаемой информации	Используется СЗИ от НСД утратившее сертификат	низкая вероятность (2)	средняя (0,35)	Реализация угрозы может привести к нарушению целостности и доступности защищаемой информации.	средняя	**актуальная**
Несанкционированное восстановление удаленной защищаемой информации	Используется СЗИ от НСД утратившее сертификат. Данные не хранятся локально на АРМ.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности защищаемой информации.	средняя	неактуальная
Несанкционированный доступ к аутентификационной информации	Используется СЗИ от НСД утратившее сертификат	низкая вероятность (2)	средняя (0,35)	Реализация угрозы может привести к нарушению конфиденциально	средняя	**актуальная**

				сти защищаемой информации.		
Несанкционированные изменения аутентификационной информации	Используется СЗИ от НСД утратившее сертификат	низкая вероятность (2)	средняя (0,35)	Реализация угрозы может привести к нарушению целостности и доступности защищаемой информации.	средняя	**актуальная**
Удаление аутентификационной информации	Используется СЗИ от НСД утратившее сертификат	низкая вероятность (2)	средняя (0,35)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации.	средняя	**актуальная**
Угроза обхода некорректно настроенных механизмов аутентификации	Используется СЗИ от НСД утратившее сертификат	средняя вероятность (5)	средняя (0,5)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации.	средняя	**актуальная**

Продолжение приложения Б

Несанкционированное создание учетной записи пользователей	Используется СЗИ от НСД утратившее сертификат.	средняя вероятность (5)	средняя (0,5)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации.	средняя	**актуальная**
Угроза Несанкционированного использования системных и сетевых утилит	Используется СЗИ от НСД утратившее сертификат	средняя вероятность (5)	средняя (0,5)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации.	средняя	**актуальная**
Избыточное выделение оперативной памяти	Используется средство антивирусной защиты и СЗИ от НСД утратившее сертификат	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению доступности защищаемой информации.	низкая	неактуальная
Использование информации идентификации/	Учетные записи «по умолчанию» отключены.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению	средняя	неактуальная

Продолжение приложения Б

аутентификации, заданной по умолчанию				конфиденциальности, целостности и доступности защищаемой информации.		
Использование механизмов авторизации для повышения привилегий	Используется СЗИ от НСД утратившее сертификат	средняя вероятность (5)	средняя (0,5)	Реализация угрозы может привести к нарушению конфиденциальности защищаемой информации.	средняя	**актуальная**
Несанкционированное редактирование реестра	Используется СЗИ от НСД утратившее сертификат.	средняя вероятность (5)	средняя (0,5)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации.	средняя	**актуальная**
Использование поддельных цифровых подписей BIOS	Получение прошивки BIOS происходит только из надёжных источников.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности	средняя	неактуальная

				защищаемой информации.		
Несанкционированное использование привилегированных функций BIOS	Получение прошивки BIOS происходит только из надёжных источников.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации.	средняя	неактуальная
Установка уязвимых версий обновления программного обеспечения BIOS	Обновление прошивки BIOS происходит своевременно, чаще всего обновления не выпускаются много лет.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации.	средняя	неактуальная
Некорректное использование функционала программного обеспечения	Используется СЗИ от НСД утратившее сертификат.	средняя вероятность (5)	средняя (0,5)	Реализация угрозы может привести к нарушению конфиденциальности, доступности защищаемой информации.	средняя	**актуальная**

Продолжение приложения Б

Продолжение приложения Б

Нарушение целостности данных кеша	Используется СЗИ от НСД утратившее сертификат.	средняя вероятность (5)	средняя (0,5)	Реализация угрозы может привести к нарушению целостности и доступности защищаемой информации.	средняя	**актуальная**
Нарушение целостности данных кеша	Используется СЗИ от НСД утратившее сертификат.	средняя вероятность (5)	средняя (0,5)	Реализация угрозы может привести к нарушению конфиденциальности, целостности защищаемой информации.	средняя	**актуальная**
Обнаружение открытых портов и идентификации привязанных к ним сетевых служб	Используется СЗИ от НСД утратившее сертификат.	низкая вероятность (2)	средняя (0,35)	Реализация угрозы может привести к нарушению конфиденциальности информации.	средняя	**актуальная**
Обнаружение хостов	Используется СЗИ от НСД утратившее сертификат.	низкая вероятность (2)	средняя (0,35)	Реализация угрозы может привести к нарушению конфиденциальности информации.	средняя	**актуальная**

Продолжение приложения Б

Определение типов объектов защиты и получение предварительной информации об объекте защиты	Используется СЗИ от НСД утратившее сертификат.	средняя вероятность (5)	средняя (0,5)	Реализация угрозы может привести к нарушению конфиденциальности информации.	средняя	**актуальная**
Удаленный подбор аутентификацион-ных данных пользователя	Используется СЗИ от НСД утратившее сертификат.	низкая вероятность (2)	средняя (0,35)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности информации.	средняя	**актуальная**
Удаленное внедрение вредоносных программ	Используется средство антивирусной защиты. Порядок организации антивирусной защиты регламентирован.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности информации	средняя	неактуальная
Перехват данных, передаваемых по вычислительной сети «прослушивание сетевого трафика»	Используются средства криптографической защиты информации.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности защищаемой информации.	средняя	неактуальная

Продолжение приложения Б

Подмена доверенного пользователя	Используются средства криптографической защиты информации.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности защищаемой информации.	средняя	неактуальная
Угроза «фарминга»	Предусмотрены инструкции пользователей.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности защищаемой информации.	средняя	неактуальная
Угроза «фишинга»	Используется средство антивирусной защиты. Предусмотрены инструкции пользователей.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности защищаемой информации.	средняя	неактуальная
Подмена субъекта сетевого доступа «имитация действий сервера»	Используются средства криптографической защиты информации.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности информации	средняя	неактуальная

Продолжение приложения Б

Преднамеренные действия внутреннего нарушителя						
Аппаратный сброс пароля BIOS	Ремонт, обслуживание и сопровождение программных, технических и программно-технических средств ИС, в том числе СЗИ, выполняется администратором ИС. В помещении, в котором происходит обработка защищаемой информации, исключено неконтролируемое пребывание посторонних лиц.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению целостности защищаемой информации. Системные блоки ПЭВМ не опломбированы.	средняя	неактуальная
Программный сброс пароля BIOS	Полномочия пользователей по установке ПО ограничены средствами СЗИ от НСД, утратившей сертификат.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности защищаемой информации.	средняя	неактуальная

Продолжение приложения Б

Подбор пароля BIOS	В ИС установлены пароли на BIOS. Предусмотрена парольная политика.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности и доступности защищаемой информации.	средняя	неактуальная
Внедрение вредоносного кода в BIOS	Ремонт и обслуживание технических средств ИС осуществляется силами администратора ИС. Используется средство антивирусной защиты.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации.	средняя	неактуальная
Восстановление предыдущей уязвимой версии BIOS	Ремонт и обслуживание технических средств ИС осуществляется силами администратора ИС. Пользователи не имеют прав	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации.	средняя	неактуальная

Продолжение приложения Б

	администратора при работе на ПЭВМ.					
Установка уязвимых версий обновления программного обеспечения BIOS	В ИС установлены пароли на BIOS. Пользователи не имеют прав администратора при работе на ПЭВМ. Ремонт и обслуживание технических средств ИС осуществляется силами администратора ИС.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации.	средняя	неактуальная
Деструктивное использование декларированного функционала BIOS	Администратор ИС осуществляет периодический контроль защищенности ИС и контроль за действиями пользователей. Уязвимости программного обеспечения BIOS не обнаружены.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению целостности защищаемой информации.	средняя	неактуальная

Продолжение приложения Б

	В ИС установлены пароли на BIOS.					
Нарушение изоляции среды исполнения BIOS	Администратор ИС осуществляет периодический контроль защищенности ИС и контроль за действиями пользователей	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации.	средняя	неактуальная
Угроза невозможности управления правами пользователей BIOS	Пользователи не имеют прав администратора при работе на ПЭВМ. В ИС установлены пароли на BIOS. Пользователям не требуется вносить изменения в настройки BIOS в рамках исполнения должностных полномочий	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации.	средняя	неактуальная
Несанкционированное выключение или обход механизма	В ИС установлены пароли на BIOS. Ремонт и обслуживание	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению	средняя	неактуальная

Продолжение приложения Б

защиты от записи в BIOS	технических средств ИС осуществляется силами администратора ИС. Пользователи не имеют прав администратора при работе на ПЭВМ			конфиденциальности, целостности и доступности защищаемой информации.		
Несанкционированное использование привилегированных функций BIOS	В ИС установлены пароли на BIOS. Ремонт и обслуживание технических средств ИС осуществляется силами администратора ИС Пользователи не имеют прав администратора при работе на ПЭВМ.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации.	средняя	неактуальная
Подмена резервной копии программного обеспечения BIOS	В ИС установлены пароли на BIOS. Пользователи не имеют прав администратора при работе на ПЭВМ.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению целостности защищаемой	средняя	неактуальная

Продолжение приложения Б

	Ремонт и обслуживание технических средств ИС осуществляется силами администратора ИС.			информации.		
Несанкционированное управление буфером	Пользователи не имеют прав администратора при работе на ПЭВМ.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности защищаемой информации.	средняя	неактуальная
Преднамеренное изменение или уничтожение программных компонентов ИС	Пользователи не имеют прав администратора при работе на ПЭВМ. Полномочия пользователей по установке ПО ограничены СЗИ от НСД, утратившим сертификат.	низкая вероятность (2)	средняя (0,35)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации.	средняя	**актуальная**
Внедрение программных закладок	Используется средство антивирусной	низкая вероятность (2)	средняя (0,35)	Реализация угрозы может привести к	средняя	**актуальная**

Продолжение приложения Б

	защиты ИС. Полномочия пользователей по установке ПО ограничены СЗИ от НСД, утратившим сертификат.			нарушению конфиденциальности, целостности и доступности защищаемой информации.		
Перехват вводимой и выводимой на периферийные устройства информации	Используется средство антивирусной защиты.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности защищаемой информации.	средняя	неактуальная
Загрузка нештатной операционной системы	В ИС установлены пароли на BIOS. В ИС запрещена загрузка операционной системы со съемных носителей информации	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации.	средняя	неактуальная
Внедрение вредоносных программ	Используется средство антивирусной защиты ИС.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности	средняя	неактуальная

				и доступности защищаемой информации. Порядок организации антивирусной защиты не регламентирован. Обновление базы антивирусной программы не регламентировано.		
Угроза эксплуатации цифровой подписи программного кода	Используется средство антивирусной защиты ИС.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности, доступности защищаемой информации.	средняя	неактуальная
Подделка записей журнала регистрации событий	Полномочия пользователей по доступу к журналам регистрации событий ограничены	низкая вероятность (2)	средняя (0,35)	Реализация угрозы может привести к нарушению целостности защищаемой	средняя	**актуальная**

Продолжение приложения Б

	ограничены СЗИ от НСД, утратившим сертификат.			информации.		
Несанкционированное изменение параметров настройки средств защиты информации	Пользователи не имеют прав администратора при работе на ПЭВМ.	низкая вероятность (2)	средняя (0,35)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации.	средняя	**актуальная**
Несанкционированный доступ к информации с применением стандартных функций операционной системы (уничтожение, копирование, перемещение и т. п.)	Пользователи не имеют прав администратора при работе на ПЭВМ.	низкая вероятность (2)	средняя (0,35)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации.	средняя	**актуальная**
Несанкционированный доступ к информации с использованием прикладного	Пользователи не имеют прав администратора при работе на ПЭВМ.	низкая вероятность (2)	средняя (0,35)	Реализация угрозы может привести к нарушению конфиденциальности, целостности	средняя	**актуальная**

Продолжение приложения Б

программного обеспечения				и доступности защищаемой информации.		
Несанкционированный доступ к информации с использованием специально созданного программного обеспечения	Типовой состав ПО не включает средства создания программного обеспечения. Пользователи не имеют прав администратора при работе на ПЭВМ.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации.	средняя	неактуальная
Неправомерное ознакомление с защищаемой информацией	В ИС реализовано разграничение доступа к защищаемой информации средствами СЗИ от НСД, утратившим сертификат и организационными мерами.	низкая вероятность (2)	средняя (0,35)	Реализация угрозы может привести к нарушению конфиденциальности защищаемой информации.	средняя	**актуальная**
Несанкционированная модификация защищаемой информации	В ИС реализовано разграничение доступа к защищаемой информации средствами СЗИ от НСД, утратившим	низкая вероятность (2)	средняя (0,35)	Реализация угрозы может привести к нарушению целостности защищаемой информации..	средняя	**актуальная**

Продолжение приложения Б

	сертификат и организационными мерами.					
Использование слабостей кодирования входных данных	В ИС реализовано разграничение доступа к защищаемой информации средствами ограничены СЗИ от НСД, утратившим сертификат и организационными мерами. Пользователи не имеют прав администратора при работе на ПЭВМ.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению целостности и доступности защищаемой информации.	средняя	неактуальная
Несанкционированное копирование информации на внешние (сменные) носители	Предусмотрены инструкции пользователей.	низкая вероятность (2)	средняя (0,35)	Реализация угрозы приведет к нарушению конфиденциальности защищаемой информации. Порядок использования сменных носителей	средняя	**актуальная**

				информации не . регламентирован		
Подбор аутентификацион-ных данных пользователя	Предусмотрена парольная политика.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации.	средняя	неактуальная
Несанкционированный доступ к аутентификационной информации	В ИС реализовано разграничение доступа к защищаемой информации средствами СЗИ от НСД, утратившим сертификат и организационными мерами. Предусмотрена парольная политика.	низкая вероятность (2)	средняя (0,35)	Реализация угрозы может привести к нарушению конфиденциальности защищаемой информации.	средняя	**актуальная**
Несанкционированные изменения аутентификационной информации	В ИС реализовано разграничение доступа к защищаемой информации	низкая вероятность (2)	средняя (0,35)	Реализация угрозы может привести к нарушению целостности и	низкая	**актуальная**

Продолжение приложения Б

	средствами СЗИ от НСД, утратившим сертификат и организационными мерами. Предусмотрена парольная политика.			доступности защищаемой информации.		
Удаление аутентификационной информации	В ИС реализовано разграничение доступа к защищаемой информации средствами СЗИ от НСД, утратившим сертификат и организационными мерами. Предусмотрена парольная политика.	низкая вероятность (2)	средняя (0,35)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации.	средняя	**актуальная**
Угроза обхода некорректно настроенных механизмов аутентификации	В ИС реализовано разграничение доступа к защищаемой информации средствами СЗИ от НСД, утратившим сертификат и	низкая вероятность (2)	средняя (0,35)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой	средняя	**актуальная**

Продолжение приложения Б

	организационными мерами.			информации.		
Использование информации идентификации/ аутентификации, заданной по умолчанию	Учетные записи «по умолчанию» отключены.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации.	средняя	неактуальная
Использование механизмов авторизации для повышения привилегий	В ИС реализовано разграничение доступа к защищаемой информации средствами СЗИ от НСД, утратившим сертификат.	низкая вероятность (2)	средняя (0,35)	Реализация угрозы может привести к нарушению конфиденциальности защищаемой информации.	средняя	**актуальная**
Удаление защищаемой информации	В ИС реализовано разграничение доступа к защищаемой информации средствами СЗИ от НСД, утратившим сертификат.	низкая вероятность (2)	средняя (0,35)	Реализация угрозы может привести к нарушению доступности защищаемой информации.	средняя	**актуальная**

Продолжение приложения Б

Несанкционированное восстановление удаленной защищаемой информации	В ИС реализовано разграничение доступа к защищаемой информации средствами СЗИ от НСД, утратившим сертификат.	средняя вероятность (5)	средняя (0,5)	Реализация угрозы может привести к нарушению конфиденциальности защищаемой информации.	средняя	**актуальная**
Несанкционированное создание учетной записи пользователей	Пользователи не имеют прав администратора при работе на ПЭВМ. В ИС реализовано разграничение доступа к защищаемой информации средствами СЗИ от НСД, утратившим сертификат и организационными мерами.	средняя вероятность (5)	средняя (0,5)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации.	средняя	**актуальная**
Несанкционированное редактирование реестра	Пользователи не имеют прав администратора при работе на ПЭВМ. В ИС реализовано разграничение доступа к	средняя вероятность (5)	средняя (0,5)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности	средняя	**актуальная**

	защищаемой информации средствами СЗИ от НСД, утратившим сертификат и организационными мерами.			защищаемой информации.		
Повреждение системного реестра	Пользователи не имеют прав администратора при работе на ПЭВМ. В ИС реализовано разграничение доступа к защищаемой информации средствами СЗИ от НСД, утратившим сертификат и организационными мерами.	средняя вероятность (5)	средняя (0,5)	Реализация угрозы может привести к нарушению целостности и доступности защищаемой информации.	средняя	**актуальная**
Угроза Несанкционированного использования системных и сетевых утилит	Пользователи не имеют прав администратора при работе на ПЭВМ. В ИС реализовано разграничение доступа к защищаемой	средняя вероятность (5)	средняя (0,5)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой	средняя	**актуальная**

	информации средствами СЗИ от НСД, утратившим сертификат и организационными мерами.			информации.		
Угроза подмены программного обеспечения	Права пользователей по установке ПО ограничены.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации.	средняя	неактуальная
Изменение режимов работы или отключение средств защиты информации	Доступ к настройке средств защиты имеет только администратор ИС.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации.	средняя	неактуальная
Избыточное выделение оперативной памяти	Используются средства антивирусной защиты.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению доступности	средняя	неактуальная

Продолжение приложения Б

				защищаемой информации.		
Изменение компонентов системы	Пользователи не имеют прав администратора при работе на ПЭВМ. В ИС реализовано разграничение доступа к защищаемой информации средствами СЗИ от НСД, утратившим сертификат.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению целостности и доступности защищаемой информации.	средняя	неактуальная
Изменение режимов работы аппаратных элементов компьютера	Доступ к настройкам BIOS ограничен.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению целостности и доступности защищаемой информации.	средняя	неактуальная
Исследование механизмов работы программы	Пользователи не имеют прав администратора при работе на ПЭВМ. Доступ к дистрибутивам ПО ограничен.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, доступности защищаемой	средняя	неактуальная

				информации.		
Перехват привилегированного процесса	Пользователи не имеют прав администратора при работе на ПЭВМ.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации.	средняя	неактуальная
Непреднамеренные действия внутреннего нарушителя						
Непреднамеренный запуск вредоносных программ	Используется средство антивирусной защиты ИС. Порядок организации антивирусной защиты регламентирован.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации.	средняя	неактуальная
Непреднамеренная модификация (уничтожение) информации	Доступ пользователей к защищаемой информации ограничен в рамках служебных обязанностей.	низкая вероятность (2)	средняя (0,35)	Реализация угрозы может привести к нарушению целостности и доступности защищаемой информации.	средняя	**актуальная**

Продолжение приложения Б

Непреднамеренное изменение или уничтожение программных компонентов ИС	Пользователи не имеют прав администратора при работе на ПЭВМ.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации.	средняя	неактуальная
Непреднамеренное изменение режимов работы или отключение средств защиты информации	Доступ к настройке средств защиты имеет только администратор ИС.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации.	средняя	неактуальная
Утрата ключевой/парольной информации	Регламентирован порядок организации парольной защиты. Предусмотрены инструкции пользователей ИС.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации.	средняя	неактуальная
Локальные уязвимости системного программного обеспечения						

Недекларированные возможности системного программного обеспечения	Пользователи не имеют прав администратора при работе на ПЭВМ.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой информации.	средняя	неактуальная
Угроза сбоя процесса обновления BIOS	Обслуживание технических средств ИС осуществляет администратор ИС.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению доступности защищаемой информации.	средняя	неактуальная
Несанкционированное повышение привилегий пользователя операционной системы	В ИС реализовано разграничение доступа к защищаемой информации СЗИ от НСД, утратившим сертификат.	низкая вероятность (2)	средняя (0,35)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности ПДн.	средняя	**актуальная**
Несанкционированное выполнение произвольных команд	В ИС реализовано разграничение доступа к защищаемой информации СЗИ от	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциально	средняя	неактуальная

Продолжение приложения Б

операционной системы	НСД, утратившим сертификат.			сти, целостности и доступности ПДн.		
Модификация (подмена) компонентов операционной системы	Пользователи ИС не обладают полномочиями администратора. Используются средства антивирусной защиты.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности ПДн.	средняя	неактуальная
Отказ в обслуживании операционной системы	Уязвимости отказа в обслуживании операционной системы не обнаружены.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению целостности и доступности ПДн.	средняя	неактуальная
Локальные уязвимости прикладного программного обеспечения						
Недекларированные возможности прикладного программного обеспечения	Пользователи не имеют прав администратора при работе на ПЭВМ.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности защищаемой	средняя	неактуальная

				информации.		
Несанкционированное повышение привилегий пользователя	В ИС реализовано разграничение доступа к защищаемой информации СЗИ от НСД, утратившим сертификат.	низкая вероятность (2)	средняя (0,35)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности ПДн.	средняя	**актуальная**
Несанкционированное выполнение произвольных команд операционной системы через уязвимости прикладного программного обеспечения	Уязвимости несанкционированного выполнения произвольных команд операционной системы не обнаружены.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности ПДн.	средняя	неактуальная
Модификация (подмена) компонентов прикладного программного обеспечения	Используются средства антивирусной защиты. Пользователи не имеют прав администратора при работе на ПЭВМ.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению конфиденциальности, целостности и доступности ПДн.	средняя	неактуальная

Продолжение приложения Б

Отказ в обслуживании прикладного программного обеспечения	В ходе обследования уязвимости отказа в обслуживании прикладного программного обеспечения не обнаружены.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению целостности и доступности ПДн.	средняя	неактуальная
Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	В ходе обследования уязвимости микропрограммного обеспечения средств хранения, обработки и (или) ввода/вывода/передачи информации не обнаружены.	маловероятно (0)	низкая (0,25)	Реализация угрозы может привести к нарушению целостности и доступности ПДн.	низкая	неактуальная
Угрозы персонала						
Преднамеренное разглашение конфиденциальной информации	Обязанность соблюдать конфиденциальность информации закреплена в локальных документах Таможенного управления.	маловероятно (0)	низкая (0,25)	Реализация угрозы приведет к нарушению конфиденциальности защищаемой информации.	средняя	неактуальная

Продолжение приложения Б

Непреднамеренное разглашение конфиденциальной информации	Обязанность соблюдать конфиденциальность информации закреплена в локальных документах Таможенного управления.	маловероятно (0)	низкая (0,25)	Реализация угрозы приведет к нарушению конфиденциальности защищаемой информации.	средняя	неактуальная
Допуск за рабочее место лиц, не имеющих на это право	Предусмотрены локальные документы Таможенного управления, регламентирующие порядок доступа к ИС. Неконтролируемое нахождение посторонних лиц в помещении, где осуществляется обработка защищаемой информации не допускается.	маловероятно (0)	низкая (0,25)	Реализация угрозы приведет к нарушению конфиденциальности, целостности, доступности защищаемой информации.	низкая	неактуальная

Таким образом, в отношении информации, обрабатываемой в ИС Таможенного управления, актуальными являются следующие угрозы безопасности:

1. **Угрозы несанкционированного доступа с применением программно-аппаратных средств (в том числе программно-математических воздействий)**
   - 1.1.Преднамеренные действия внешнего нарушителя
     - 1.1.1. Подделка записей журнала регистрации событий
     - 1.1.2. Несанкционированное изменение параметров настройки средств защиты информации
     - 1.1.3. Доступ к защищаемым файлам с использованием альтернативных путей доступа к ресурсам
     - 1.1.4. Несанкционированная модификация защищаемой информации
     - 1.1.5. Несанкционированное удаление защищаемой информации
     - 1.1.6. Несанкционированный доступ к аутентификационной информации
     - 1.1.7. Несанкционированные изменения аутентификационной информации
     - 1.1.8. Удаление аутентификационной информации
     - 1.1.9. Угроза обхода некорректно настроенных механизмов аутентификации
     - 1.1.10. Несанкционированное создание учетной записи пользователей
     - 1.1.11. Угроза Несанкционированного использования системных и сетевых утилит
     - 1.1.12. Использование механизмов авторизации для повышения привилегий
     - 1.1.13. Несанкционированное редактирование реестра
     - 1.1.14. Некорректное использование функционала программного обеспечения
     - 1.1.15. Нарушение целостности данных кеша
     - 1.1.16. Нарушение целостности данных кеша
     - 1.1.17. Обнаружение открытых портов и идентификации привязанных к ним сетевых служб
     - 1.1.18. Обнаружение хостов
     - 1.1.19. Определение типов объектов защиты и получение предварительной информации об объекте защиты
     - 1.1.20. Удаленный подбор аутентификационных данных пользователя
   - 1.2.Преднамеренные действия внутреннего нарушителя
     - 1.2.1. Преднамеренное изменение или уничтожение программных компонентов ИС
     - 1.2.2. Внедрение программных закладок
     - 1.2.3. Подделка записей журнала регистрации событий
     - 1.2.4. Несанкционированное изменение параметров настройки средств защиты информации

1.2.5. Несанкционированный доступ к информации с применением стандартных функций операционной системы (уничтожение, копирование, перемещение и т. п.)
1.2.6. Несанкционированный доступ к информации с использованием прикладного программного обеспечения
1.2.7. Неправомерное ознакомление с защищаемой информацией
1.2.8. Несанкционированная модификация защищаемой информации
1.2.9. Несанкционированное копирование информации на внешние (сменные) носители
1.2.10. Несанкционированный доступ к аутентификационной информации
1.2.11. Несанкционированные изменения аутентификационной информации
1.2.12. Удаление аутентификационной информации
1.2.13. Угроза обхода некорректно настроенных механизмов аутентификации
1.2.14. Использование механизмов авторизации для повышения привилегий
1.2.15. Удаление защищаемой информации
1.2.16. Несанкционированное восстановление удаленной защищаемой информации
1.2.17. Несанкционированное создание учетной записи пользователей
1.2.18. Несанкционированное редактирование реестра
1.2.19. Повреждение системного реестра
1.2.20. Угроза несанкционированного использования системных и сетевых утилит
1.3.Непреднамеренные действия внутреннего нарушителя
1.3.1. Несанкционированное повышение привилегий пользователя операционной системы
1.4.Локальные уязвимости прикладного программного обеспечения
1.4.1. Несанкционированное повышение привилегий пользователя

ПРИЛОЖЕНИЕ В

УТВЕРЖДАЮ
Начальник Таможенного управления

_____

«_____»_____2017 г.

ТРЕБОВАНИЯ
к системе защиты информации в
информационной системе персональных данных «ОПСУР»
Таможенного управления

ОБЩИЕ ПОЛОЖЕНИЯ

Основными **целями** обеспечения защиты информации в информационной системе (далее – ИС) являются:

– обеспечение необходимого уровня защищенности ИС в соответствии с требованиями нормативных документов ФСТЭК России и ФСБ России;

– снижение вероятности реализации актуальных угроз информационной безопасности;

– проведение процедуры оценки соответствия (аттестации) ИС.

Объектами защиты ИС являются:

– ИС в целом;

– НЖМД (стационарные и съемные);

– файлы (в т.ч. временные и технологические) на автоматизированных рабочих местах ИС и каталоги с файлами, содержащие защищаемую информацию;

– файлы (в т.ч. временные и технологические) на сервере ИС и каталоги с файлами, содержащие защищаемую информацию, расположенную в базе данных;

– каталоги (файлы) с общесистемным и прикладным программным обеспечением;

– каталог (файлы) системы защиты информации от несанкционированного доступа (далее – СЗИ от НСД);

– мониторы с отображаемой на них информацией;

– каталоги всех файлов;

– оперативная память ПЭВМ;

– операционная система ПЭВМ;

– программы, предназначенные для обработки информации;

– программные средства, осуществляющие функции по защите информации на ПЭВМ.

Данные требования по обеспечению безопасности информации при ее обработке в информационной системе персональных данных «ОПСУР» (далее – ИС) разработаны на основании:

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

2) 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 персональных данных»;

3) приказа ФСТЭК России от 11 февраля 2013 г. №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

4) «Модели угроз и модель нарушителя безопасности информации ограниченного доступа, в том числе персональных данных, при ее обработке в информационной системе «Бухгалтерский учет».

Требования определяют совокупность организационных, правовых и технических мероприятий, необходимых для обеспечения заданного уровня безопасности информации при ее обработке в ИС. Требования распространяются только на данную ИС.

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», ИС присваивается 4 (четвертый) уровень защищенности.

ОРГАНИЗАЦИОННЫЕ МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Для ИС необходимо:

– организовать режим обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

– привести в соответствие с текущим законодательством по защите информации имеющиеся организационно-распорядительные документы;

– утвердить перечень лиц, доступ которых к информации, обрабатываемой в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

– назначить должностное лицо (работника), ответственного за обеспечение безопасности информации в информационной системе.

ТЕХНИЧЕСКИЕ МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

В ходе разработки требований к системе защиты информации в ИС были проведены следующие этапы:

– Определение базового набора мер.
– Адаптация базового набора мер.
– Уточнение адаптированного базового набора мер.
– Дополнение уточненного адаптированного базового набора мер.

Определение базового набора мер

На основании установленного 4-го уровня защищенности ИС, в соответствии с приказом ФСТЭК России от 18 февраля 2013 г. №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению

Продолжение приложения Б

безопасности персональных данных при их обработке в информационных системах персональных данных» и с учетом требований установленных приказом ФСТЭК России от 11 февраля 2013 г. №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

Условное обозначение меры	Мера по обеспечению безопасности
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
ИАФ.5	Защита обратной связи при вводе аутентификационной информации
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)
II. Управление доступом субъектов доступа к объектам доступа (УПД)	
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы

УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)
III. Ограничение программной среды (ОПС)	
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов
IV. Защита машинных носителей информации (ЗНИ)	
ЗНИ.1	Учет машинных носителей информации
ЗНИ.2	Управление доступом к машинным носителям информации
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)
V. Регистрация событий безопасности (РСБ)	
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения

РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе
РСБ.7	Защита информации о событиях безопасности
VI. Антивирусная защита (АВЗ)	
АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)	
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе
IX. Обеспечение целостности информационной системы и информации (ОЦЛ)	
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций
XI. Защита среды виртуализации (ЗСВ)	

ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей
XII. Защита технических средств (ЗТС)	
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования
ЗТС.3	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
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи

ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе
ЗИС.30	Защита мобильных технических средств, применяемых в информационной системе

Продолжение приложения Б

Адаптация базового набора мер

В рамках проведения адаптации базового набора мер для ИС, на основании анализа структурно-функциональных характеристик информационной системы, информационных технологий, особенностей функционирования информационной системы, было осуществлено исключение из базового набора тех мер, применение которых в данной информационной системе не требуется ввиду технологических особенностей ИС.

Исключенные меры:

Условное обозначение меры	Мера по обеспечению безопасности
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)
II. Управление доступом субъектов доступа к объектам доступа (УПД)	
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)
XI. Защита среды виртуализации (ЗСВ)	
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре

ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи
ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе
ЗИС.30	Защита мобильных технических средств, применяемых в информационной системе

Уточнение адаптированного базового набора мер

На основании частной модели угроз безопасности информации при ее обработке в ИС были выявлены следующие актуальные угрозы:

1. **Угрозы несанкционированного доступа с применением программно-аппаратных средств (в том числе программно-математических воздействий)**

1.1. Преднамеренные действия внешнего нарушителя

1.1.1. Подделка записей журнала регистрации событий

1.1.2. Несанкционированное изменение параметров настройки средств защиты информации

1.1.3. Доступ к защищаемым файлам с использованием альтернативных путей доступа к ресурсам

1.1.4. Несанкционированная модификация защищаемой информации

1.1.5. Несанкционированное удаление защищаемой информации

1.1.6. Несанкционированный доступ к аутентификационной информации

1.1.7. Несанкционированные изменения аутентификационной информации

1.1.8. Удаление аутентификационной информации

1.1.9. Угроза обхода некорректно настроенных механизмов аутентификации

1.1.10. Несанкционированное создание учетной записи пользователей

1.1.11. Угроза Несанкционированного использования системных и сетевых утилит

1.1.12. Использование механизмов авторизации для повышения привилегий

1.1.13. Несанкционированное редактирование реестра

1.1.14. Некорректное использование функционала программного обеспечения

1.1.15. Нарушение целостности данных кеша

1.1.16. Нарушение целостности данных кеша

1.1.17. Обнаружение открытых портов и идентификации привязанных к ним сетевых служб

1.1.18. Обнаружение хостов

1.1.19. Определение типов объектов защиты и получение предварительной информации об объекте защиты

1.1.20. Удаленный подбор аутентификационных данных пользователя

1.2. Преднамеренные действия внутреннего нарушителя

1.2.1. Преднамеренное изменение или уничтожение программных компонентов ИС

1.2.2. Внедрение программных закладок

1.2.3. Подделка записей журнала регистрации событий

1.2.4. Несанкционированное изменение параметров настройки средств защиты информации

1.2.5. Несанкционированный доступ к информации с применением стандартных функций операционной системы (уничтожение, копирование, перемещение и т. п.)

1.2.6. Несанкционированный доступ к информации с использованием прикладного программного обеспечения

1.2.7. Неправомерное ознакомление с защищаемой информацией

1.2.8. Несанкционированная модификация защищаемой информации

1.2.9. Несанкционированное копирование информации на внешние (сменные) носители

1.2.10. Несанкционированный доступ к аутентификационной информации

1.2.11. Несанкционированные изменения аутентификационной информации

1.2.12. Удаление аутентификационной информации

1.2.13. Угроза обхода некорректно настроенных механизмов аутентификации

1.2.14. Использование механизмов авторизации для повышения привилегий

1.2.15. Удаление защищаемой информации

1.2.16. Несанкционированное восстановление удаленной защищаемой информации

1.2.17. Несанкционированное создание учетной записи пользователей

1.2.18. Несанкционированное редактирование реестра

1.2.19. Повреждение системного реестра

1.2.20. Угроза несанкционированного использования системных и сетевых утилит

1.3. Непреднамеренные действия внутреннего нарушителя

1.3.1. Несанкционированное повышение привилегий пользователя операционной системы

1.4. Локальные уязвимости прикладного программного обеспечения

1.4.1. Несанкционированное повышение привилегий пользователя

Все актуальные угрозы нейтрализуется базовыми мерами.

Дополнение уточненного адаптированного базового набора мер

Для обеспечения передачи персональных данных в сторонние организации по сетям связи общего пользования (интернет) должны быть использованы сертифицированные ФСБ средства криптографической защиты информации. Порядок использования средств криптографической защиты информации должен быть регламентирован.

Окончательно определенные требования к системе защиты персональных данных

На основании вышеизложенного, сформированы окончательные требования к системе защиты информации:

Условное обозначение меры	Мера по обеспечению безопасности
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
ИАФ.5	Защита обратной связи при вводе аутентификационной информации
II. Управление доступом субъектов доступа к объектам доступа (УПД)	
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами

УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
III. Ограничение программной среды (ОПС)	
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов
IV. Защита машинных носителей информации (ЗНИ)	
ЗНИ.1	Учет машинных носителей информации
ЗНИ.2	Управление доступом к машинным носителям информации
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)
V. Регистрация событий безопасности (РСБ)	
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них

РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе
РСБ.7	Защита информации о событиях безопасности
VI. Антивирусная защита (АВЗ)	
АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)	
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе
IX. Обеспечение целостности информационной системы и информации (ОЦЛ)	
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций
X. Обеспечение доступности информации (ОДТ)	
ОДТ.4	Периодическое резервное копирование информации на резервные машинные носители информации
ОДТ.5	Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала
XII. Защита технических средств (ЗТС)	

ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования
ЗТС.3	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
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр

ПРИЛОЖЕНИЕ Г

УТВЕРЖДАЮ
Начальник Таможенного управления

_____

«_____»_____2017 г.

Должностная инструкция
лица, ответственного за организацию обработки персональных данных в Таможенном управлении

1. Общие положения

1.1 Настоящая Инструкция разработана в соответствии со следующими нормативными правовыми актами:

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

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

– Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.2 Ответственное лицо за организацию обработки персональных данных – лицо, отвечающее за организацию обработки персональных данных с использованием средств автоматизации и без использования таких средств, а также доступ к персональным данным Таможенного управления.

1.3 Ответственный за организацию обработки персональных данных назначается распоряжением Таможенного управления.

1.4 Ответственный за организацию обработки персональных данных в своей деятельности должен руководствоваться Трудовым кодексом РФ, Кодексом РФ об административных правонарушениях, Федеральным законом от 27.07.2006г № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006г № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлением Правительства РФ от 15.09.2008г № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства РФ от 21.03.2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», постановлением Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных», правовыми актами Таможенного управления в сфере обработки и хранения персональных данных, а также защиты конфиденциальной информации.

1.5 Ответственный за организацию обработки персональных данных осуществляет методическое руководство по обеспечению безопасности персональных данных и контроль выполнения требований по обеспечению безопасности персональных

данных при их обработке в Таможенном управлении дополнительно к своим непосредственным обязанностям.

2. Права и обязанности

2.1 Ответственный за организацию обработки персональных данных **ОБЯЗАН**:

2.1.1 Организовывать обработку и использование персональных данных в Таможенном управления исключительно в целях, предусмотренных нормативными правовыми актами РФ.

2.1.2 Организовывать обеспечение безопасности персональных данных требуемому уровню защищенности.

2.1.3 Осуществлять контроль содержания и объема обрабатываемых персональных данных и соответствия их перечню, утвержденному в Таможенном управлении.

2.1.4 Осуществлять внутренний контроль соблюдения требований законодательства РФ при обработке персональных данных, в том числе требований к защите персональных данных.

2.1.5 Осуществлять контроль приема и обработки запросов субъектов персональных данных или их представителей.

2.1.6 Осуществлять контроль выполнения требований организационно – распорядительных документов по обеспечению безопасности персональных при их обработке в информационных системах Таможенного управления.

2.1.7 Осуществлять контроль порядка учета, создания, хранения и использования резервных копий и машинных (выходных) документов, содержащих персональные данные.

2.1.8 Организовывать работы по контролю работоспособности технических средств защиты персональных данных, охраны объекта, средств защиты информации от несанкционированного доступа.

2.1.9 Доводить до сведения работников Таможенного управления положения, законодательства РФ о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных.

2.1.10 Проводить оценку эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных (далее – ИСПДн).

2.1.11 Вести учет лиц, допущенных к работе с персональными данными.

2.1.12 Участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн.

2.1.13 Осуществлять контроль над выполнением мероприятий по защите персональных данных.

2.1.14 Периодически представлять руководству отчет о состоянии защиты ИСПДн и о нештатных ситуациях на объектах ИСПДн и допущенных пользователями нарушениях установленных требований по защите информации.

2.1.15 Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

2.2 Ответственный за организацию обработки персональных данных **ИМЕЕТ ПРАВО**:

2.2.1 Требовать от всех пользователей информационных систем персональных данных выполнения установленной технологии обработки персональных данных, инструкций и других нормативных правовых документов по обеспечению безопасности персональных данных.

2.2.2 Запрашивать у работников Таможенного управления информацию, необходимую для реализации полномочий.

2.2.3 Требовать от уполномоченных на обработку персональных данных работников Таможенного управления уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных.

2.2.4 Требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации.

2.2.5 Участвовать в разработке мероприятий по совершенствованию безопасности персональных данных.

2.2.6 Инициировать проведение расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, модификации, порчи защищаемой информации и технических компонентов вычислительной техники.

2.2.7 Участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа.

2.2.8 Вносить руководству Таможенного управления предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства РФ в отношении обработки персональных данных или нарушения режима конфиденциальности.

2.2.9 Вносить руководству Таможенного управления предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке.

3. Ответственность

3.1 На ответственного за организацию обработки персональных данных возлагается персональная ответственность за качество проводимых им работ по обеспечению защиты персональных данных.

3.2 Ответственный за организацию обработки персональных данных несет ответственность по действующему законодательству за разглашение сведений ограниченного распространения ставших известными ему по роду работы.

ЛИСТ ОЗНАКОМЛЕНИЯ:

№ п/п	Дата	Фамилия, инициалы	Подпись

ПРИЛОЖЕНИЕ Д

УТВЕРЖДАЮ
Начальник Таможенного управления

_____

«_____»_____2017 г.

ИНСТРУКЦИЯ
по организации учета, использования и уничтожения носителей персональных данных
Таможенного управления

Общие положения

1.1 Настоящая Инструкция устанавливает основные требования к организации учета и использования носителей персональных данных в Таможенном управлении.

Организация учета и использования носителей персональных данных, возлагается на лицо, назначенное ответственным за организацию работы с персональными данными в Таможенном управлении.

1.2 Все машинные носители персональных данных подлежат обязательному учету. Допускается автоматизированный учет носителей информации.

1.3 Уничтожение носителей персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в государственной информационной системе и (или) в результате которых уничтожаются материальные носители персональных данных.

1.4 Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию: по достижении целей обработки, в случае выявления неправомерной обработки персональных данных или в случае утраты необходимости в достижении этих целей в соответствии с процедурой, предусмотренной статей 21 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

1.5 Лицами, ответственными за организацию обработки персональных данных в Таможенном управлении (далее – ответственное лицо), осуществляется систематический контроль и выделение из общей массы документов, содержащих персональные данные, подлежащие уничтожению.

1.6 Для проведения процедуры уничтожения носителей персональных данных в Таможенном управлении создается комиссия, которая в соответствии с актами об уничтожении материальных носителей персональных данных (далее – акт об уничтожении) производят уничтожение бумажных и электронных носителей персональных данных.

Учет машинных носителей информации

2.1 К машинным носителям информации относятся:

– съемные носители информации;
– несъемные жесткие магнитные диски.

2.2 Каждый машинный носитель данных, применяемый при обработке персональных данных на средствах вычислительной техники (далее – СВТ), должен иметь гриф – «Для служебного пользования».

2.3 Персональную ответственность за сохранность полученных машинных носителей данных и предотвращении несанкционированного доступа к записанной на них информации несет сотрудник, получивший эти носители.

2.4 При обработке персональных данных на СВТ должен соблюдаться следующий общий порядок учета, хранения и уничтожения машинных носителей данных.

2.4.1 Учет машинных носителей данных предназначенных для записи персональных данных производится в Журнале учета и выдачи машинных носителей данных, содержащих персональные данные (Приложение 3).

2.4.2 Каждому носителю информации присваивается учетный номер, который состоит из кода машинного носителя, номера объекта и порядкового номера по Журналу учета и выдачи машинных носителей данных, содержащих персональные данные.

2.4.3 Учетный номер и гриф «Для служебного пользования» наносятся на носитель информации или его корпус. Если невозможно маркировать непосредственно машинный носитель данных, то маркируется упаковка, в которой хранится носитель. В этом случае учетный номер записывается также на носитель машинным способом.

2.4.4 В качестве регистрационных номеров машинных носителей информации, встроенных в корпус средств вычислительной техники, используются идентификационные (серийные) номера и (или) номера инвентарного учета технических средств, имеющих встроенные носители информации. Учет встроенных в технические средства машинных

носителей информации ведется в журналах материально-технического учета в составе соответствующих технических средств.

2.4.5 Хранение машинных носителей должно осуществляться в условиях, исключающих возможность хищения, приведения в негодность или уничтожения содержащейся на них информации.

2.4.6 Машинные носители после стирания с них персональных данных, с учета не снимают, а хранятся наравне с другими машинными носителями.

2.4.7 В последующем эти носители используются для записи персональных данных. Если носители не пригодны для дальнейшего использования, они подлежат уничтожению по соответствующему акту.

2.4.8 О фактах утраты машинных носителей с грифом «Для служебного пользования» незамедлительно докладывается руководителю Таможенного управления и проводится служебное расследование.

2.4.9 Машинные носители персональных данных должны пересылаться, по возможности, в металлических коробках, помещаемых в пакет, в упаковках, конвертах тем же порядком, что и конфиденциальные документы. На пакетах, упаковках, конвертах с носителями делается надпись: «Осторожно, машинные носители информации. Не прошивать».

2.4.10 Машинные носители с персональными данными, утратившими практическое значение или пришедшие в негодность, уничтожаются по соответствующему акту (Приложение 2).

2.5 При подготовке документов должны соблюдаться следующие особенности учета, хранения и уничтожения машинных носителей данных.

2.5.1 Несъемные жесткие магнитные диски закрепляются за сотрудником, ответственным за СВТ, в котором они установлены.

2.5.2 В случае повреждения машинных носителей персональных данных, сотрудник, в пользовании которого они находятся, обязан сообщить о случившемся руководителю Таможенного управлении и ответственному за его сохранность.

2.5.3 В случае необходимости (командировка, отпуск и т. д.) машинные носители с персональными данными, сдаются сотрудником ответственному лицу на постоянное или временное хранение в опечатанном виде. При этом на упаковке указывается срок их хранения, заверенный личной подписью сотрудника. По истечению указанного срока информация может быть уничтожена, а носители могут повторно использоваться.

2.5.4 Копирование персональных данных, с машинных носителей с целью передачи другим сотрудникам производится с разрешения руководителя Таможенного управления сотрудником, постоянно работающим с данной информацией.

2.5.5 Копирование осуществляется только на тех СВТ, на которых разрешена обработка персональных данных, и только на те носители, которые соответствуют грифу «Для служебного пользования».

2.5.6 Передача скопированной информации третьим лицам производится по письменному разрешению руководства Таможенного управления.

2.5.7 Хранящиеся на магнитных носителях и потерявшие актуальность персональные данные должны своевременно стираться (уничтожаться). Ответственность за это несет владелец информации.

2.6 Руководитель Таможенного управления не реже одного раза в год инициирует проверку наличия и условий хранения персональных данных.

Уничтожение бумажных носителей персональных данных

3.1 Бумажные носители персональных данных (документы, их копии, выписки) уничтожаются путем измельчения указанных документов в специальных машинах на мелкие части, исключающие возможность последующего восстановления информации, или сжигаются.

3.2 По окончании уничтожения бумажных носителей комиссия составляет акт об уничтожении бумажных носителей персональных данных.

3.3 Акт об уничтожении бумажных носителей персональных данных составляется и подписывается комиссией в двух экземплярах (Приложение 1).

Уничтожение машинных носителей персональных данных

4.1 Машинные носители персональных данных по истечении сроков обработки и хранения на них персональных данных на основании акта об уничтожении подлежат физическому уничтожению, с целью невозможности их восстановления и дальнейшего использования, путем механического нарушения целостности носителей информации или их сжигания.

4.2 Персональные данные, хранящиеся на машинных носителях, удаляются путем стирания информации с помощью программных или технических средств, гарантирующих уничтожение информации, или путем механического нарушения целостности носителей информации.

4.3 В случае допустимости повторного использования носителя информации применяется программное удаление (затирание) содержимого путем его форматирования с последующей записью новой информации на данный носитель.

4.4 Акт об уничтожении машинных носителей персональных данных составляется и подписывается комиссией.

Акт уничтожения бумажных носителей персональных данных

Комиссия в составе:

	ФИО	Должность
Председатель		
Члены комиссии		

провела отбор бумажных носителей персональных данных и установила, что персональные данные, зафиксированные на них в процессе эксплуатации, подлежат гарантированному уничтожению:

№ п/п	Дата	Название бумажного носителя	Примечание

Всего подлежит уничтожению _____носителей.

(цифрами и прописью)

Перечисленные носители ПДн уничтожены путем _____.

(разрезания, сжигания, сдачи предприятию по утилизации вторичного сырья и т.п.)

Председатель комиссии: _____

/ /

Члены комиссии: _____

/ /

_____

/ /

_____

/ /

_____

/ /

Продолжение приложения Д
Приложение 2

Акт уничтожения машинных носителей персональных данных

Комиссия в составе:

	ФИО	Должность
Председатель		
Члены комиссии		

провела отбор носителей персональных данных, файлов и папок, содержащихся в государственной информационной системе, и установила, что персональные данные, зафиксированные на них в процессе эксплуатации, подлежат гарантированному уничтожению:

№ п/п	**Дата**	**Тип носителя**	**Регистрационный номер носителя ПДн** **Или наименование технического средства, на котором уничтожаются файлы**	**Примечание**

Всего подлежит уничтожению _____носителей.

(цифрами и прописью)

На указанных носителях персональные данные уничтожены путем _____.

(стирания на устройстве гарантированного уничтожения информации и т.п.)

Перечисленные носители ПДн уничтожены путем _____.

(разрезания, сжигания, механического уничтожения, сдачи предприятию по утилизации вторичного сырья и т.п.)

Председатель комиссии: _____

/ /

Члены комиссии: _____

/ /

_____

/ /

ПРИЛОЖЕНИЕ Е

УТВЕРЖДАЮ
Начальник Таможенного управления

_____

«_____»_____2017 г.

ТЕХНИЧЕСКИЙ ПАСПОРТ

ИНФОРМАЦИОННАЯ СИСТЕМА ПЕРСОНАЛЬНЫХ ДАННЫХ «ОПСУР»

ТАМОЖЕННОГО УПРАВЛЕНИЯ

РАЗРАБОТАЛ

Инженер отдела защиты информации
ООО «ЦЗИ «Эгида»

_____ Дьяконов А.Н.

"____" _____ 2017 г.

2017 г.

1. Общие сведения об автоматизированной системе (далее – АС)

1.1. Наименование ИСПДн: «ОПСУР» Таможенного управления.

1.2. Расположение АС:

- _____

(далее АС)

1.3. Класс АС: 4 уровень защищенности.

2. Состав оборудования АС

2.1. Перечень основных технических средств и систем, входящих в состав АС

№ п/п	Тип ОТСС	Заводской номер	Сведения по сертификации, специсследованиям и спецпроверкам
1	ПЭВМ №1, СПЗ № 1		
1.1	Системный блок HP	1013400958	-
1.2	Монитор Samsung SyncMaster 943B	1013400350	
1.3	Клавиатура HP	721720-251	-
1.4	Манипулятор «мышь» HP	672652-001	-
1.5	Принтер HP LaserJet 5000	1360678	-
1.6	Считыватель Athena IIIe	110605-067901016	-
1.7	ИБП Powerman Brick 600	571VFW11-02	-
2	ПЭВМ №2, СПЗ № 2		
2.1	Системный блок Helios Profice VLX-310	1040200455	-
2.2	Монитор Samsung SyncMaster 943B	1040200455	-
2.3	Клавиатура Defender HB-520	11647-140827-07361	-
2.4	Манипулятор «мышь» Defender DF2330B	68060115019	-
2.5	МФУ HP Laser Jet 1018	1040200129	-
2.6	Считыватель Athena IIIe	110605-067901016	-
2.7	ИБП Ippon smart power PRO 1000	FDF2302	-
3	ПЭВМ №3, СПЗ № 3		
3.1	Системный блок	10134000317	-
3.2	Монитор AOC e205Sda	10134000317	-
3.3	Клавиатура Genius GK-100011	XP11BSB10883	-
3.4	Манипулятор «мышь» Logitech B110	810-001317	-

№ п/п	Тип ОТСС	Заводской номер	Сведения по сертификации, специсследованиям и спецпроверкам
3.5	Считыватель Athena IIIe	110605-067901016	-
3.6	ИБП Powerman Brick 600	571VFW11-02	
4	ПЭВМ №4, СПЗ № 4		
4.1	Системный блок KraftWay	10549869	-
4.2	Монитор Samsung SyncMaster 943B	1040200491	-
4.3	Клавиатура KraftWay	6L83400789B	-
4.4	Манипулятор «мышь» A4tech Q3-350	-	-
4.5	Принтер Lexmor KMX611de	70167PHHOBRW6	-
4.6	Считыватель Athena IIIe	110605-067901016	-
4.7	ИБП Ippon smart power PRO 400	GFDR23T	-
5	ПЭВМ №5, Кабинет № 323		
5.1	Системный блок «НПП Системные ресурсы»	1013400100	-
5.2	Монитор Samsung SyncMaster 1940B	1013400100	-
5.3	Клавиатура Logitech	820-003902	-
5.4	Манипулятор «мышь» Logitech RX250	810-003902	-
5.5	Считыватель Athena IIIe	110605-067901016	-
5.6	ИБП APC Back-ups 650va	1086-34FGH-001	-
6	ПЭВМ №6, Кабинет № 313		
6.1	Системный блок Helios Profice VLX-310	1013400097	-
6.2	Монитор Samsung SyncMaster 1940B	1013400097	-
6.3	Клавиатура BTC	8711952	-
6.4	Манипулятор «мышь» Logitech RX-250	810-000208	-
6.5	Принтер HP LaserJet 1018	VNC3L77452	-
6.6	Считыватель Athena IIIe	110605-067901016	-
6.7	ИБП Ippon smart power PRO 400	QPTM284W	-

2.2. Перечень вспомогательных технических средств, входящих в состав АС (средств вычислительной техники, не участвующих в обработке конфиденциальной информации)

№ п/п	Тип ВТСС	Заводской номер	Примечание
1	Извещатель охранный объемный, 10 шт.	-	Кабинеты Таможенного управления
2	Извещатель пожарный дымовой оптико-электронный, 18 шт	-	
3	Извещатель охранный магнитоконтактный, 7 шт.	-	
СПЗ №1			
4	ВТСС №1		
	Системный блок DNS	0816049	
	Клавиатура Gigabyte GK-KM6150	131325014707	
	Манипулятор «мышь» Genius NetScroll 110X	X3684027107960	
	ИБП APC Smart UPS 1000	AS1319131426	
	Телефонный аппарат Panasonic KX-TS2358	0815968	
	Принтер Kyocera FS-1035MFP	б\н	
СПЗ №2			
5	ВТСС №2		
	Моноблок ProOne 600	1013401262	
	Клавиатура HP KU-1165	BDMHROC5Y761W2	
	Манипулятор «мышь» Logitech B110	LZ142HROS14	
	Сканер HP ScanJet 6000	1013401334	
	Телефонный аппарат Panasonic KX-T7730	OHBCD058632	
	Принтер Kyocera FS-1035MFP	1013401226	
	Генератор шума «Баррикада»	46SP21 072084	
6	ВТСС №3		
	Ноутбук Samsung NP-N150	ZOF93KZ300442V	
	Роутер TP-Link TL-SG 1008P	1186203902	
СПЗ №3			

7	ВТСС №4		
	Монитор AOC e205Sda	CGYC1HA027929	
	Системный блок «НПП Системные ресурсы»	0135090098	
	Клавиатура Acer KB-2971	KBKBPO309243133521 0BO	
	Манипулятор «мышь» Logitech B110	810-001317	
	Телефонный аппарат Texet TX-205M	1035016329	
	Телефонный аппарат Texet TX-205M	1035016489	
	МФУ Kyocera EcoSYS FS-1035MFP	1013400724	
	Кондиционер Deer	1060400874	
8	ВТСС №5		
	Монитор AOC e205Sda	CGYC1HA027927	
	Клавиатура Genius GK-100011	-	
	Манипулятор «мышь» Logitech B110	810-001317	
	Системный блок «НПП Системные ресурсы»	10134000426	
	Телефонный аппарат Texet TX-205	103011560	
	Принтер HP LasetJet 1018	1040200765	
СПЗ №4			
9	ВТСС №6		
	Монитор Acer AL1716F	ETL460C2607361440E4 04E	
	Клавиатура DEPO	6968201817261	
	Мышь DEPO	X800898	
	Системный блок DEPO	1040200302	
10	ВТСС №7		
	Системный блок DEPO	1040200306	
	Монитор LG 22VA53VQ	307RAVF0F271	
	Клавиатура DEPO	6968201818245	
	Мышь DEPO	156623-147	
	Считыватель Athena IIIe	10605-099370910	
	Телефон GE FS28169GE1-C	20091963	

	МФУ Xerox WorkCentre M118	49210035792	
	Кондиционер	1060300570	
11	ВТСС №8		
	Монитор Acer V193D	95205479240	
	Клавиатура KFKEA4XT	KFKEA4XT88DK0659	
	Манипулятор «мышь» Logitech M-UAE96	LZ929A60TT2	
	ИБП Emerson Libert	1013400081	
Кабинет №323			
12	ВТСС №9		
	Системный блок	104200342	
	Монитор Acer AL1716	1040200243	
	Клавиатура DNS	-	
	Манипулятор «мышь» Logitech M100	1216HC005D38	
	Принтер HP LSP2055dn	1013400667	
	Сканер HP ScanJet N6350	1040000153	
13	ВТСС №10		
	Моноблок OLDI Computers OL21MR	1013400794	
	Клавиатура Sven	SV1506MT1389	
	Манипулятор «мышь» Genius NetScroll 110	X4J8898605190	
	Факс Panasonic KX-FL423	1040500019	
	Модем ASUS RT-N16	A51EG3000608	

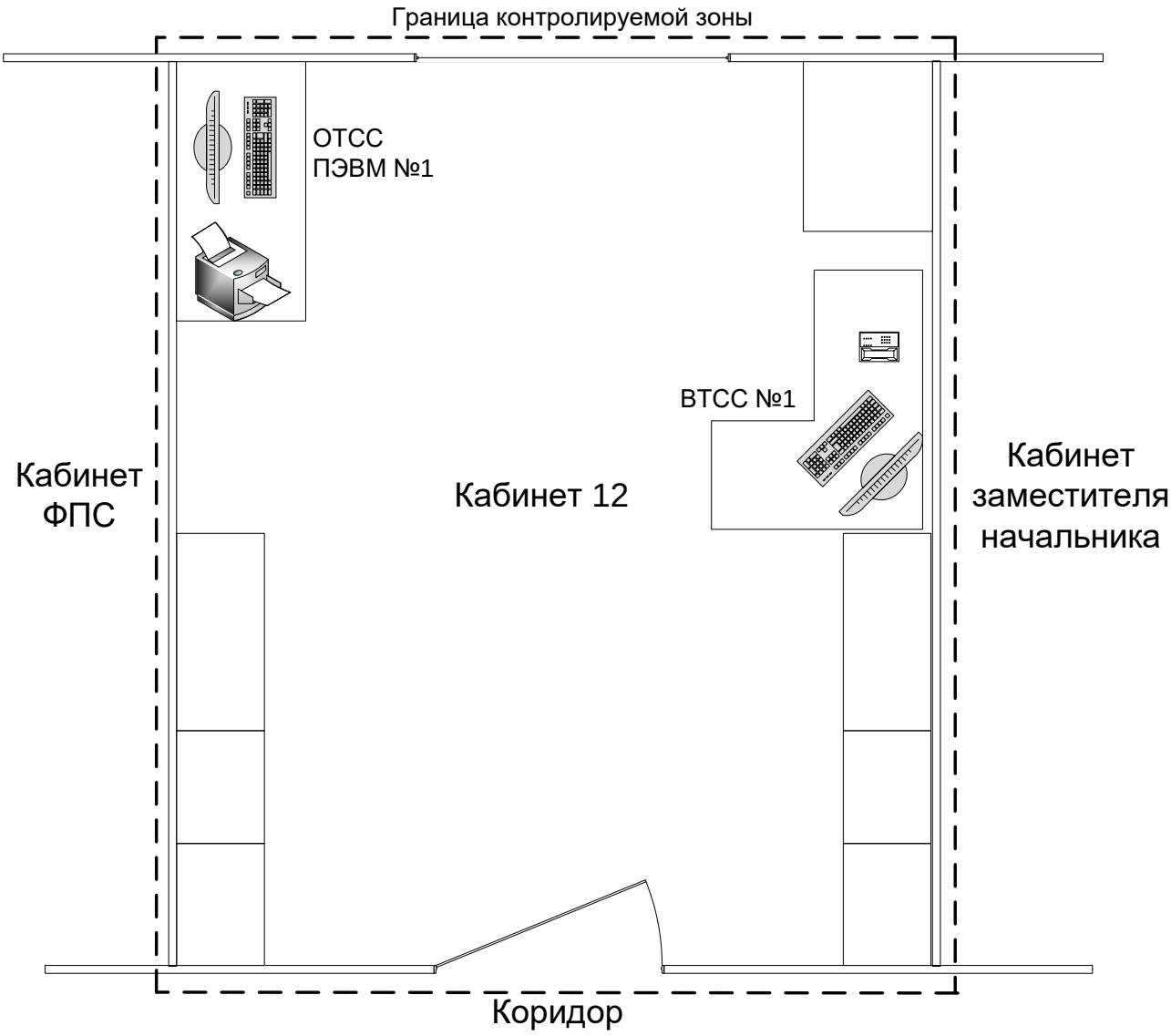
2.3. Структура, топология и размещение ОТСС относительно границ контролируемой зоны объекта:

Технические средства АИС расположены в кабинетах Таможни в частных административных зданиях. Границей контролируемой зоны являются ограждающие конструкции кабинетов Таможни. Минимальное расстояние от АС до границы контролируемой зоны составляет 1 метр.

АИС состоит из 10 АРМ пользователей, объединенных через сетевое оборудование в одноранговую ЛВС. В АИС отсутствует доступ в сеть Интернет. Обработка и хранение защищаемой информации осуществляется на сервере БДн АИС.

Структура и размещение ОТСС относительно границ контролируемой зоны приведена на Схемах 1-6.

Схема 1
служебно-производственное здание №1 , кабинет 12

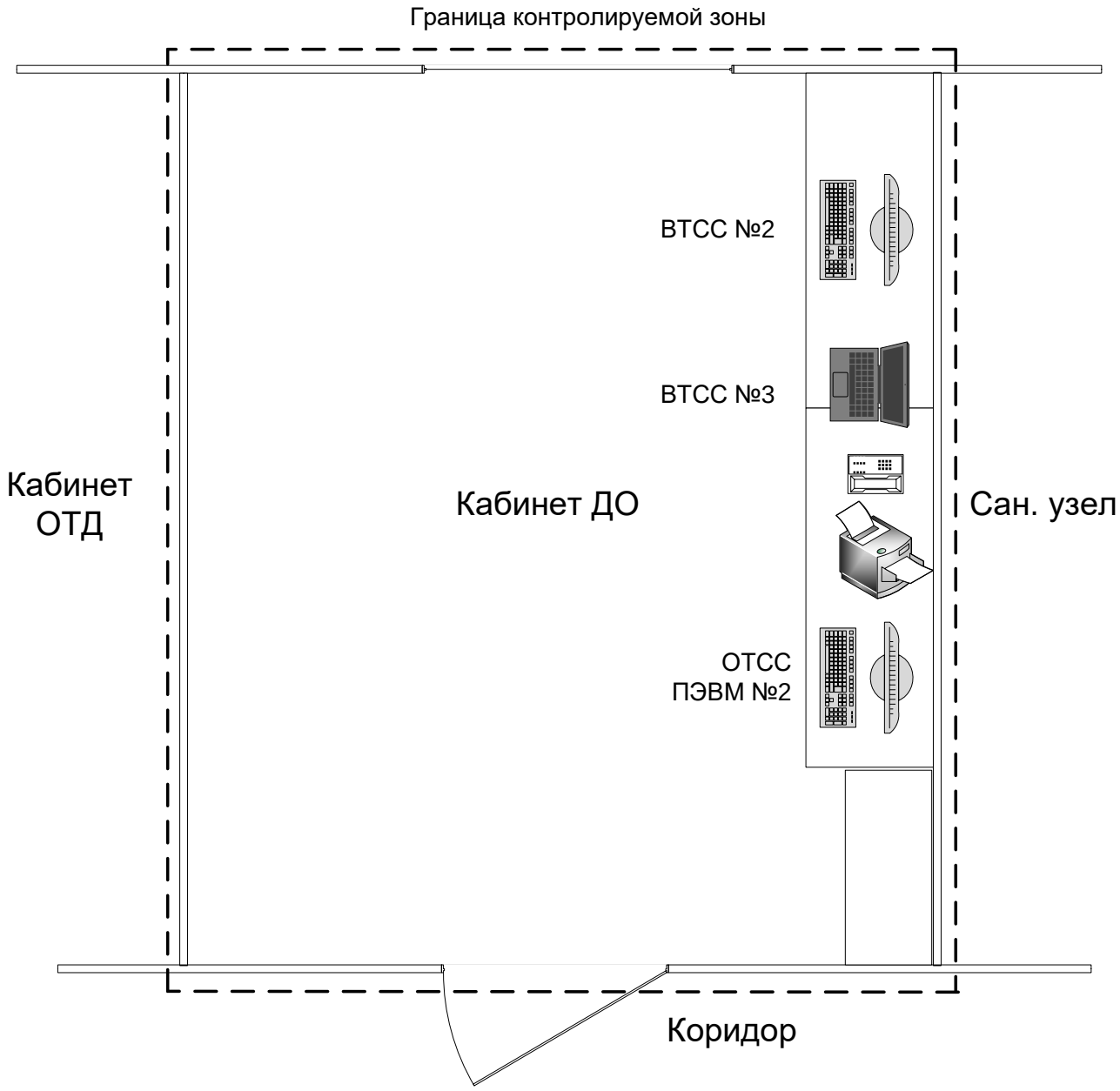


Условные обозначения:

- ПЭВМ - Принтер - Телефон

Схема 2

служебно-производственное здание №2, кабинет ДО



Условные обозначения:

- ПЭВМ - Принтер - Телефон

Схема 3

служебно-производственное здание №3, кабинет 14\2

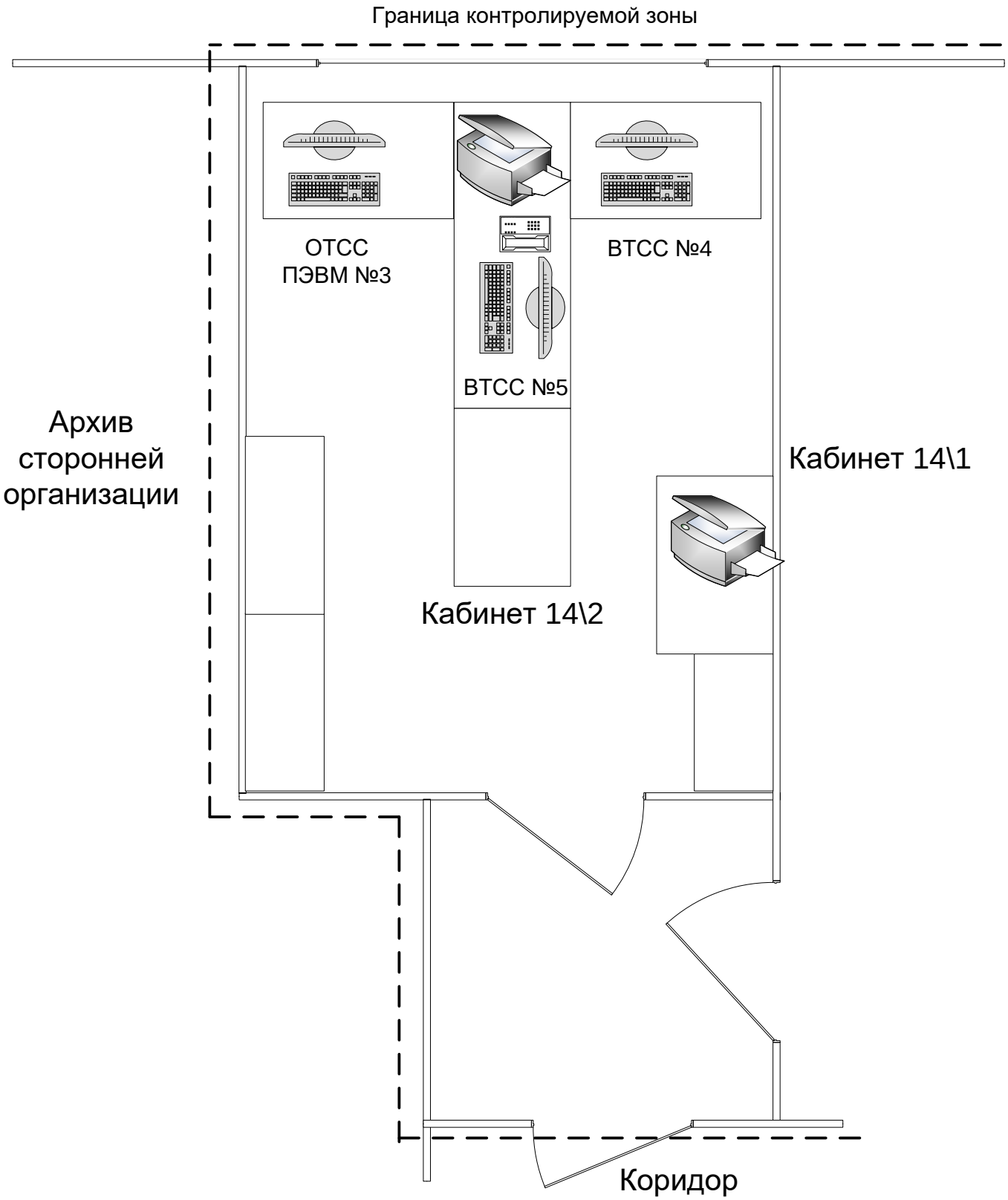
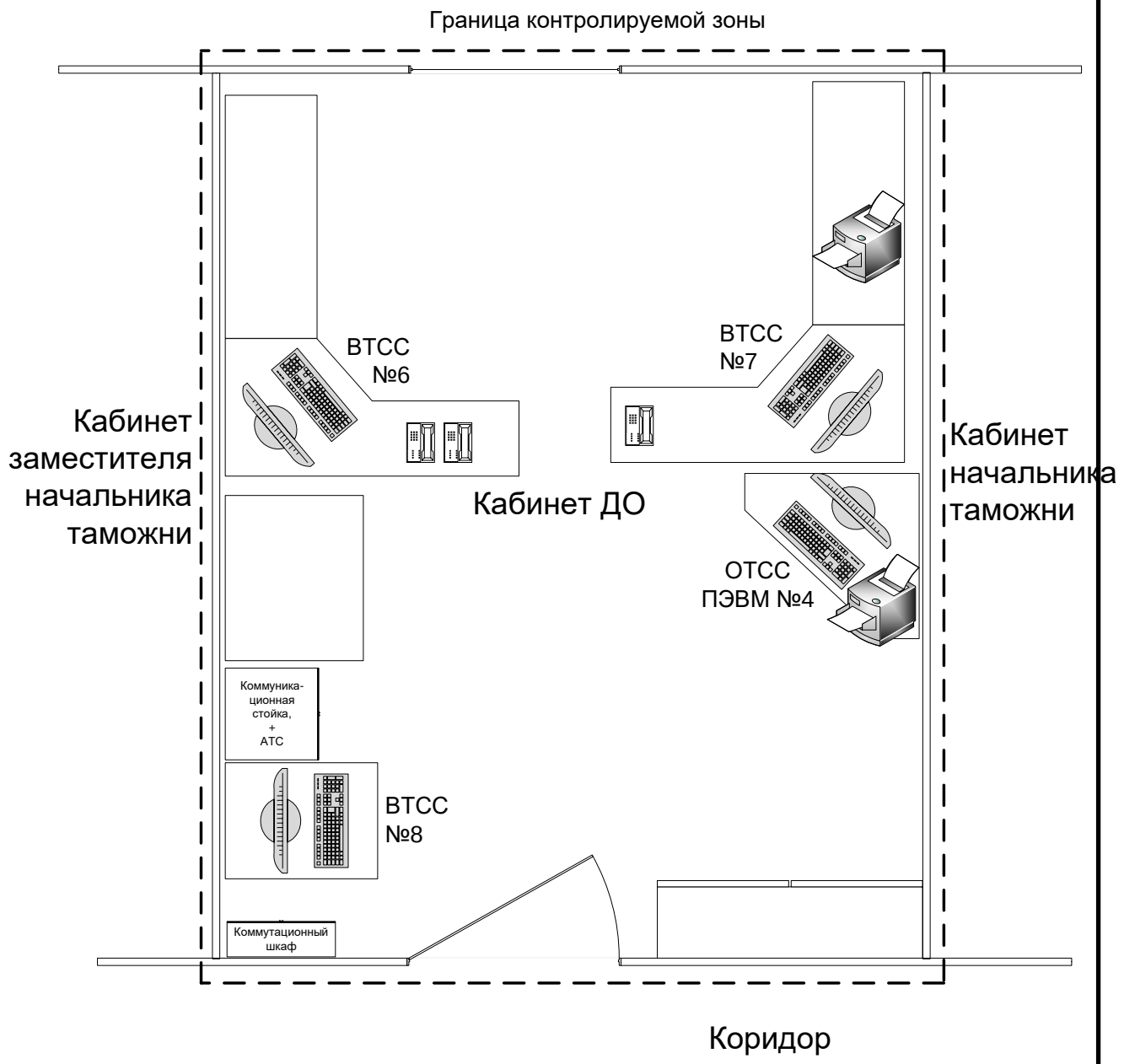


Схема 4

служебно-производственное здание №4, кабинет ДО



Условные обозначения:

- ПЭВМ

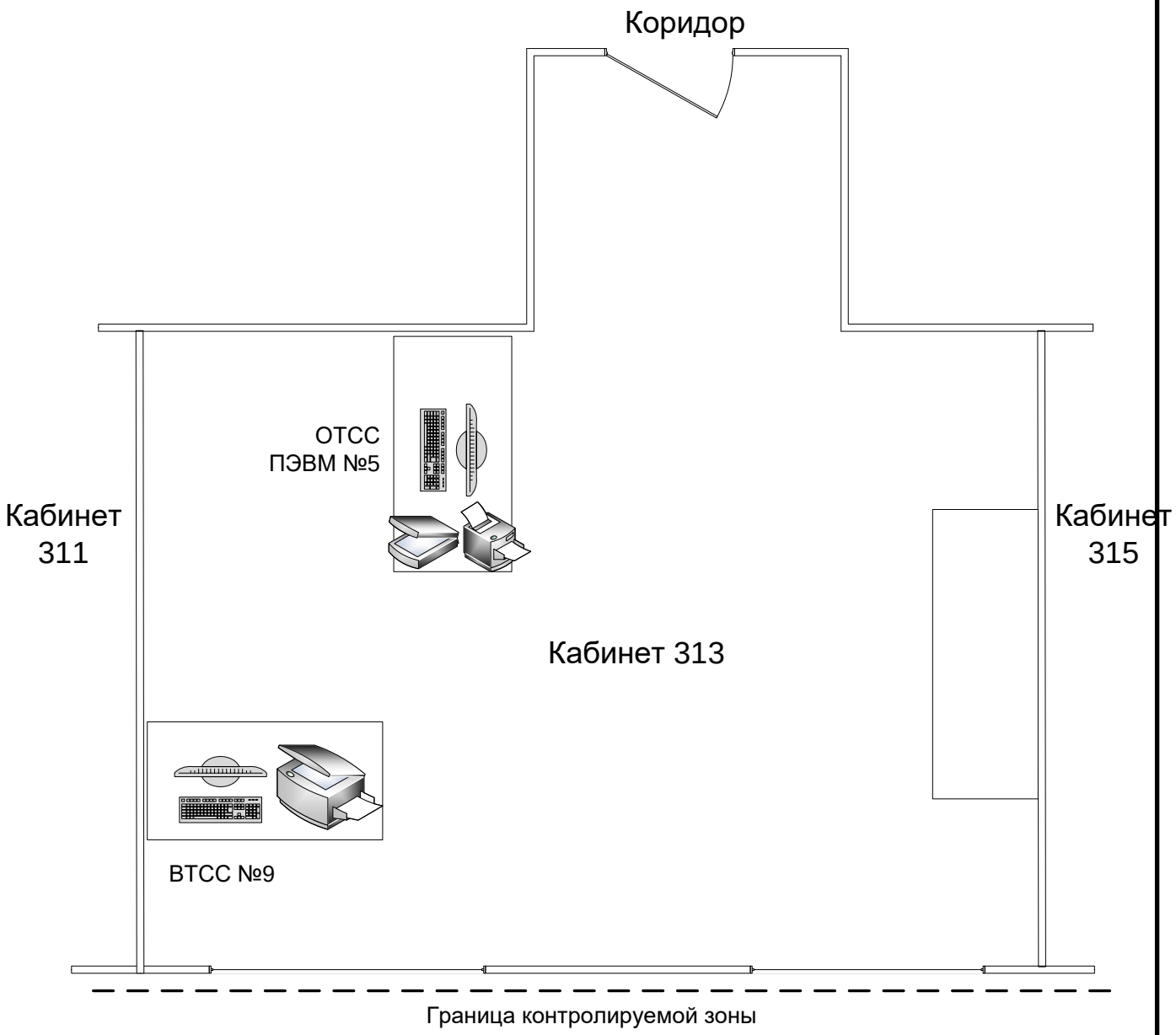
- Принтер

- Телефон

- МФУ

Схема 5

Таможенное управление кабинет № 313

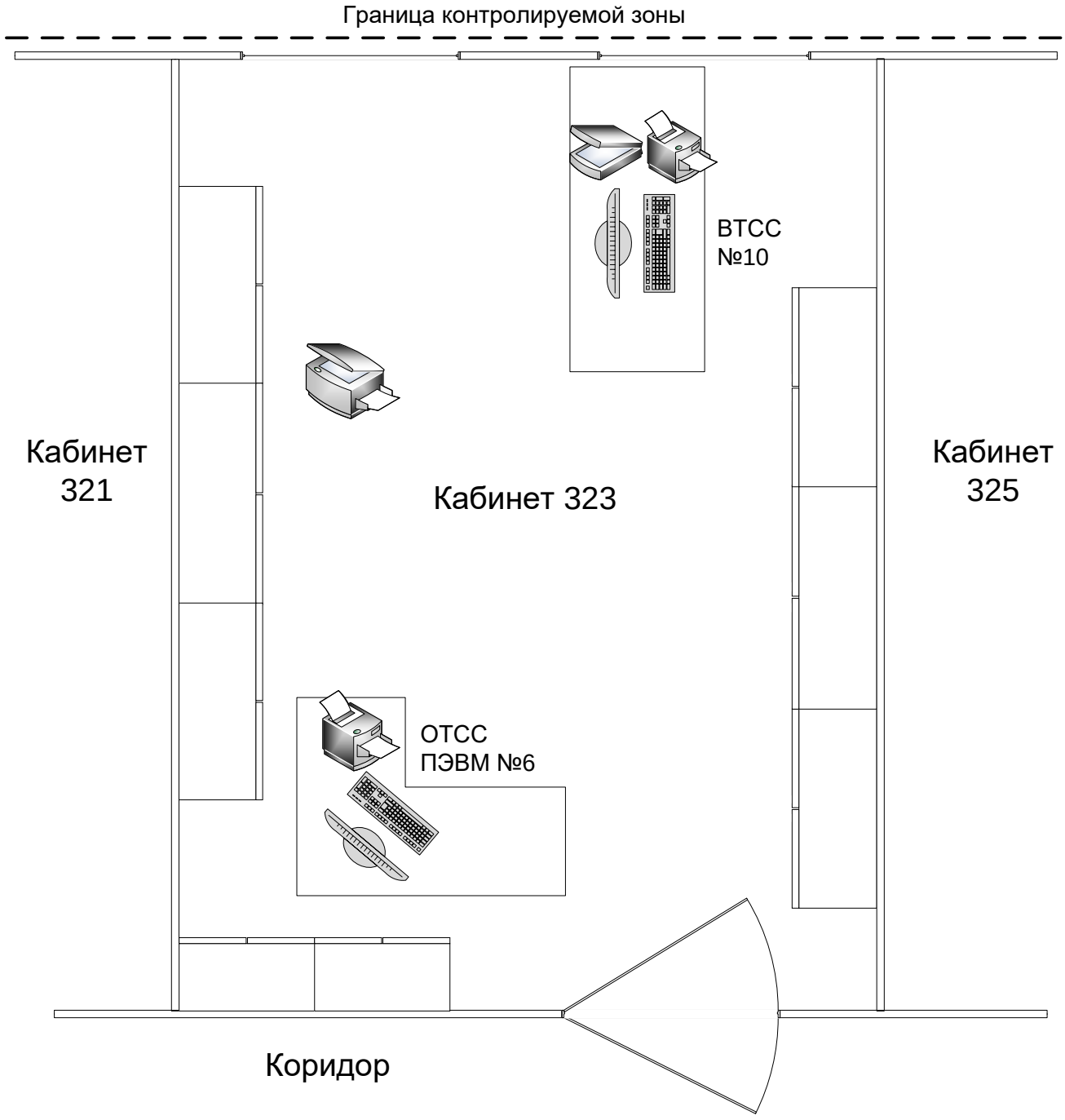


Условные обозначения:

- ПЭВМ
- Принтер
- Телефон
- МФУ
- Сканер

Схема 6

Таможенное управление, Кабинет 323



Условные обозначения:

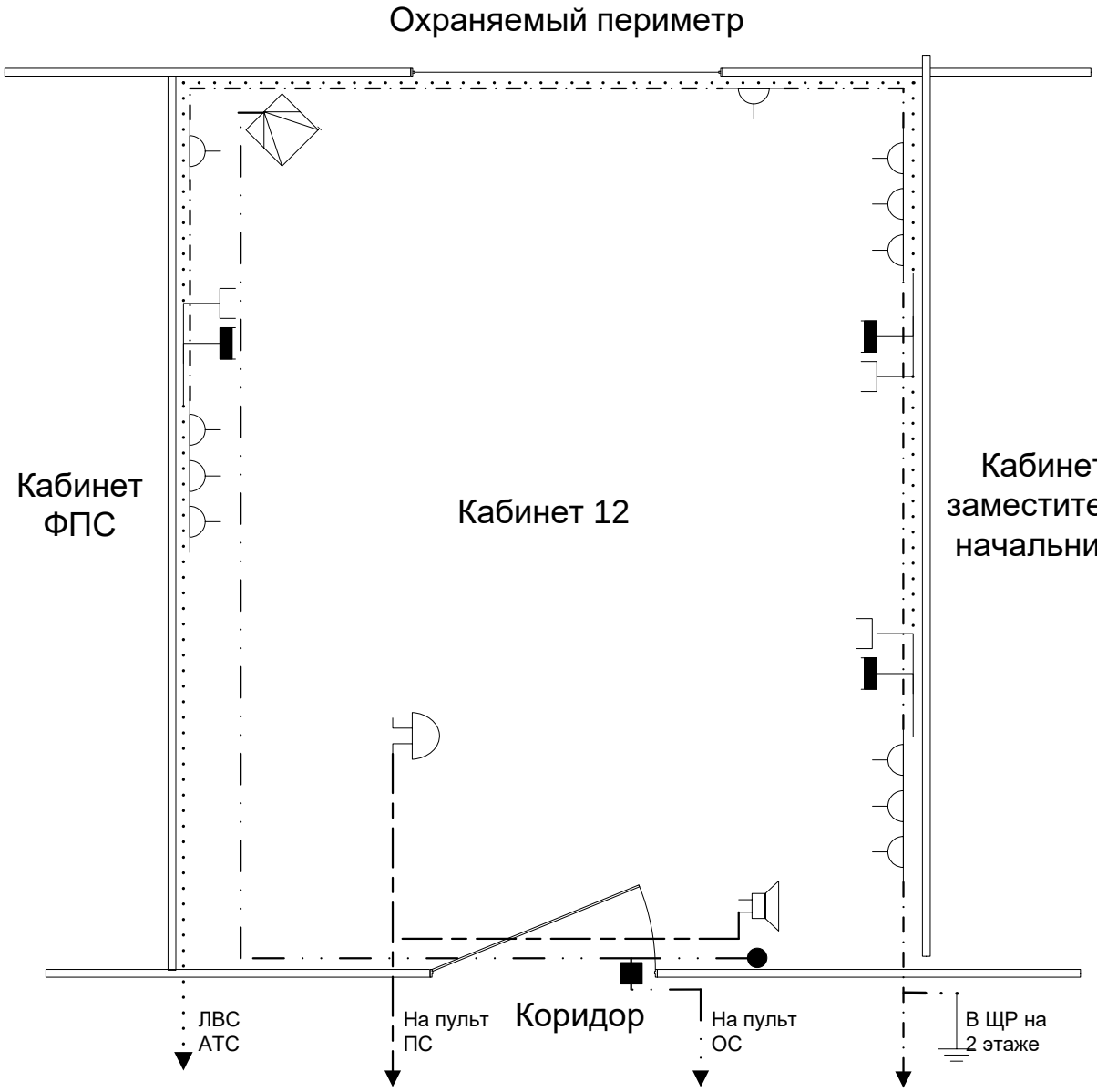
- ПЭВМ
- Принтер
- Телефон
- МФУ
- Сканер

2.4. Системы электропитания и заземления:

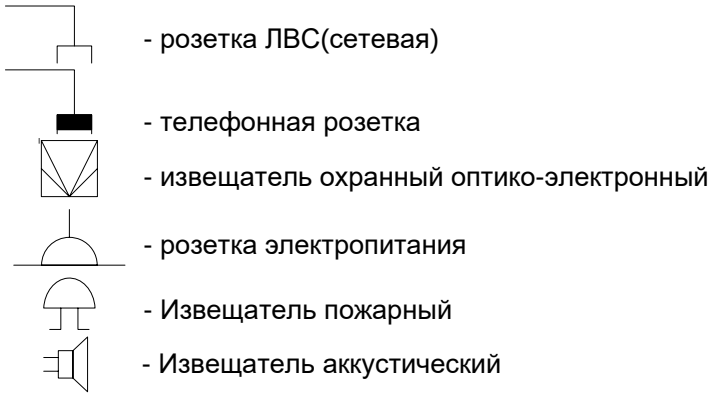
Электропитание ОТСС объекта осуществляется от распределительных щитов (ЩР), расположенных на каждом этаже зданий, за пределами контролируемых зон. Пульт охранно-пожарной сигнализации расположен на постах охраны, за пределами контролируемых зоны. Трансформаторные подстанции расположены за пределами контролируемых зоны. Схема электросети, осветительной сети и слаботочных линий представлена на схемах 7-12

Схема 7

служебно-производственное здание №1 , кабинет 12, кабинет 12



Условные обозначения:



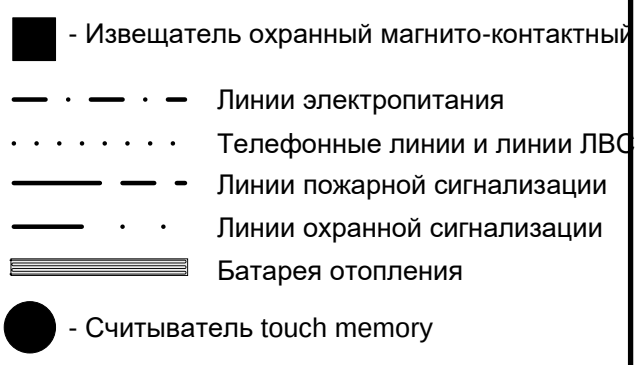
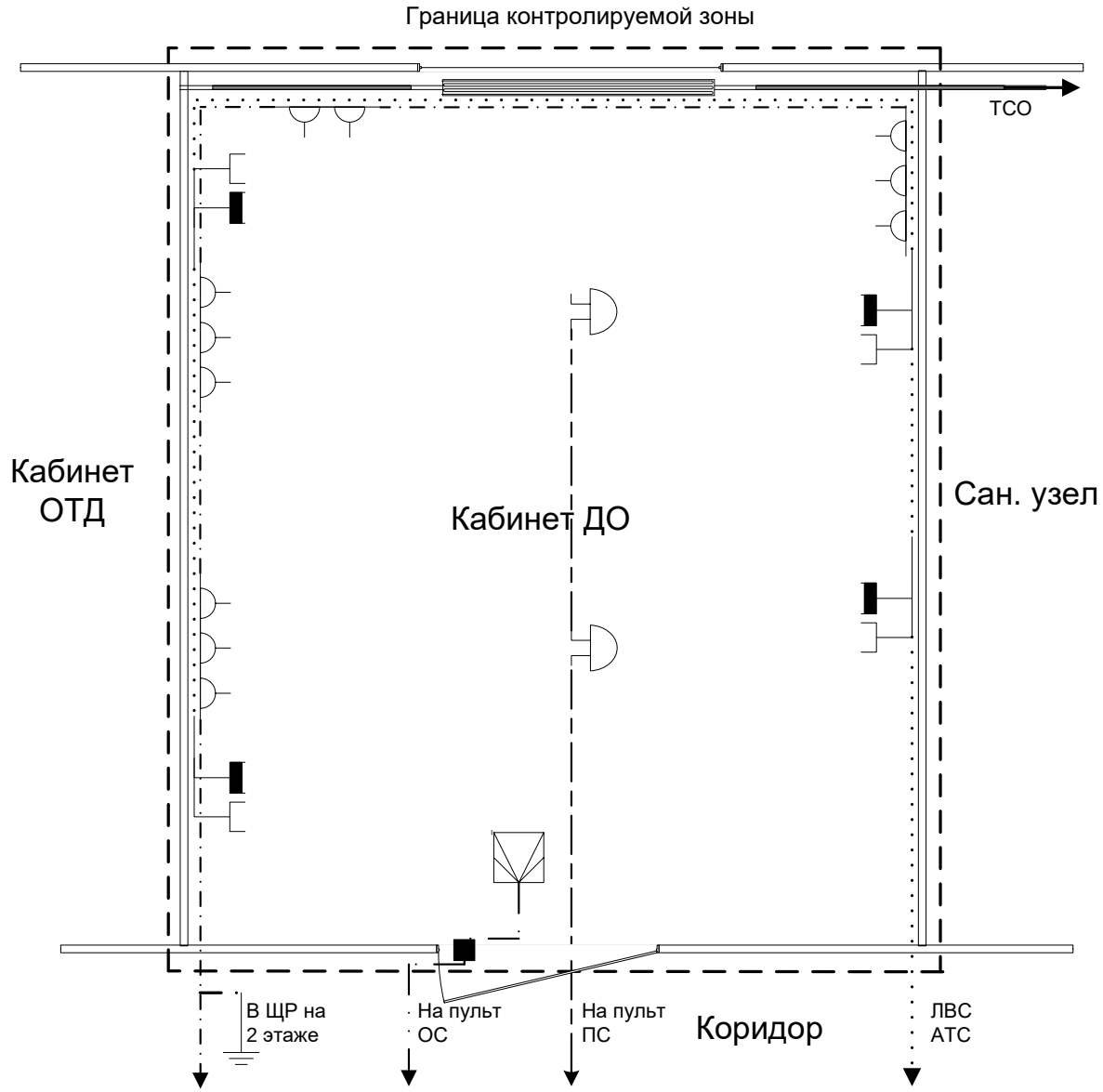


Схема 8

служебно-производственное здание №2, кабинет ДО



Условные обозначения:

- розетка ЛВС(сетевая)
- телефонная розетка
- извещатель охранный оптико-электронный
- розетка электропитания
- Извещатель пожарный
- Извещатель охранный магнито-контактный
- Линии электропитания
- Телефонные линии и линии ЛВС
- Линии пожарной сигнализации
- Линии охранной сигнализации
- Батарея отопления

Схема 9

служебно-производственное здание №3, кабинет 14\2

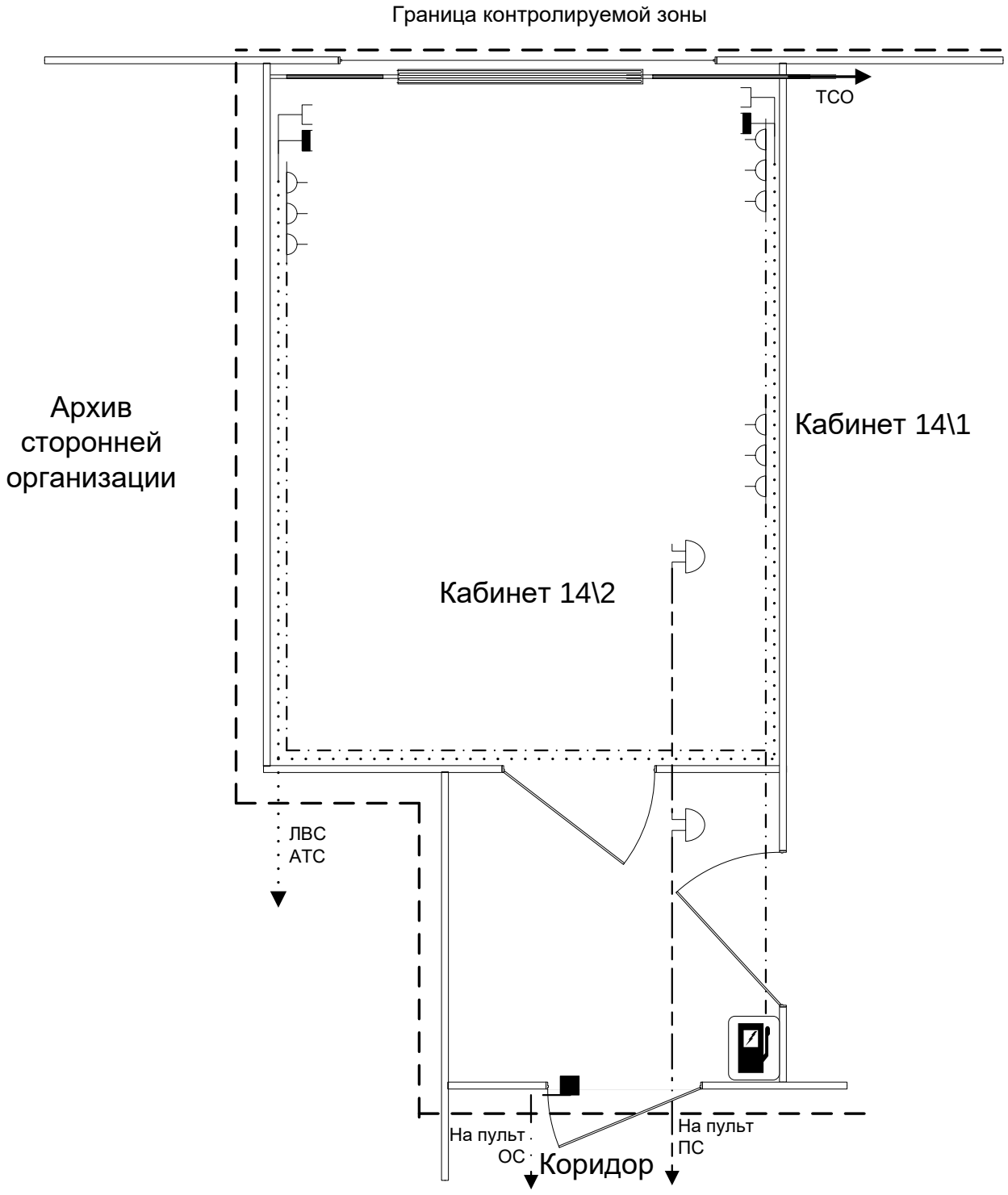
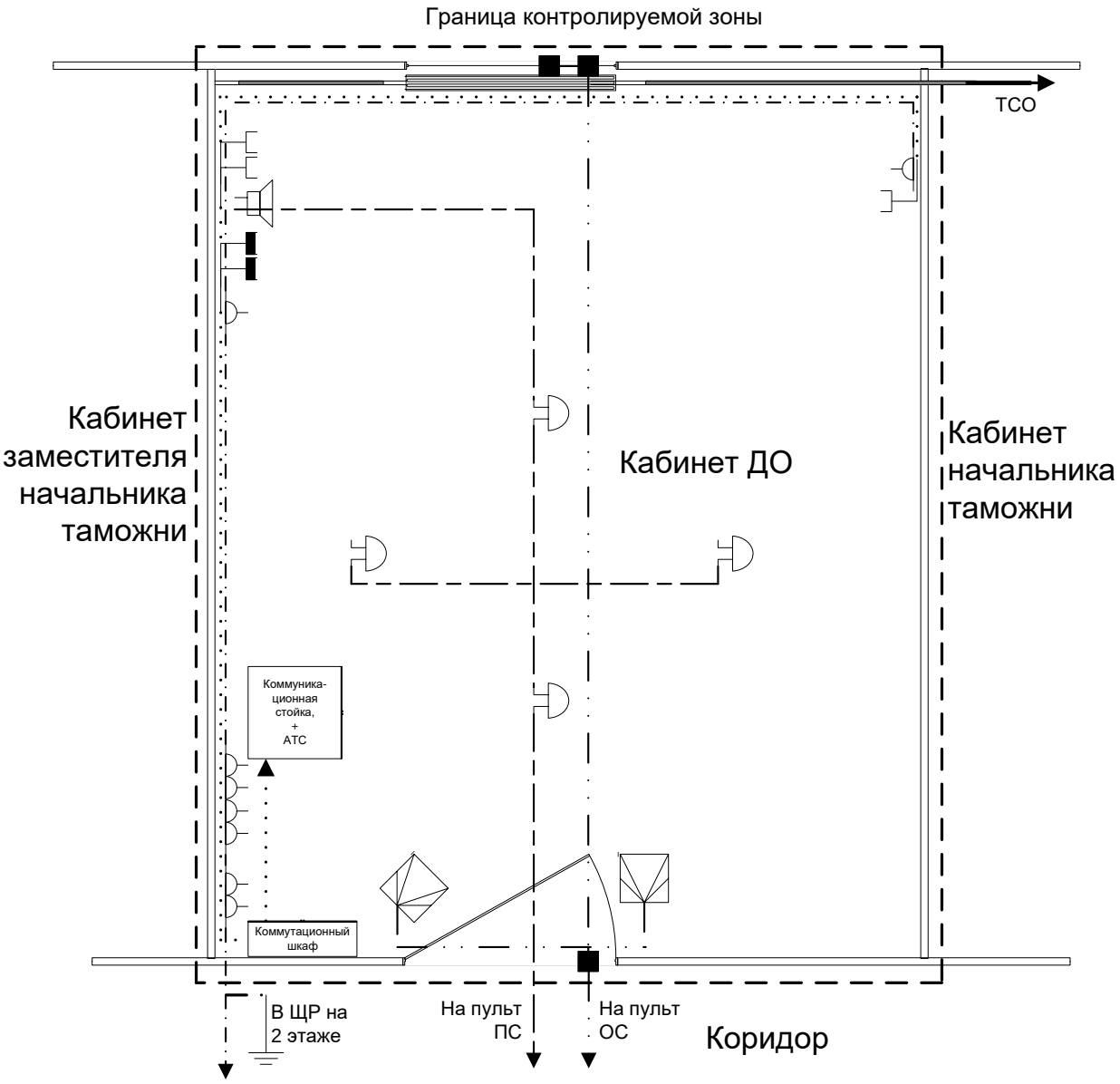


Схема 10

служебно-производственное здание №4, кабинет ДО;



Условные обозначения:

- розетка ЛВС(сетевая)
- телефонная розетка
- извещатель охранный оптико-электронный
- розетка электропитания
- Извещатель пожарный
- Извещатель охранный магнито-контактный

Линии электропитания

Телефонные линии и линии ЛВС

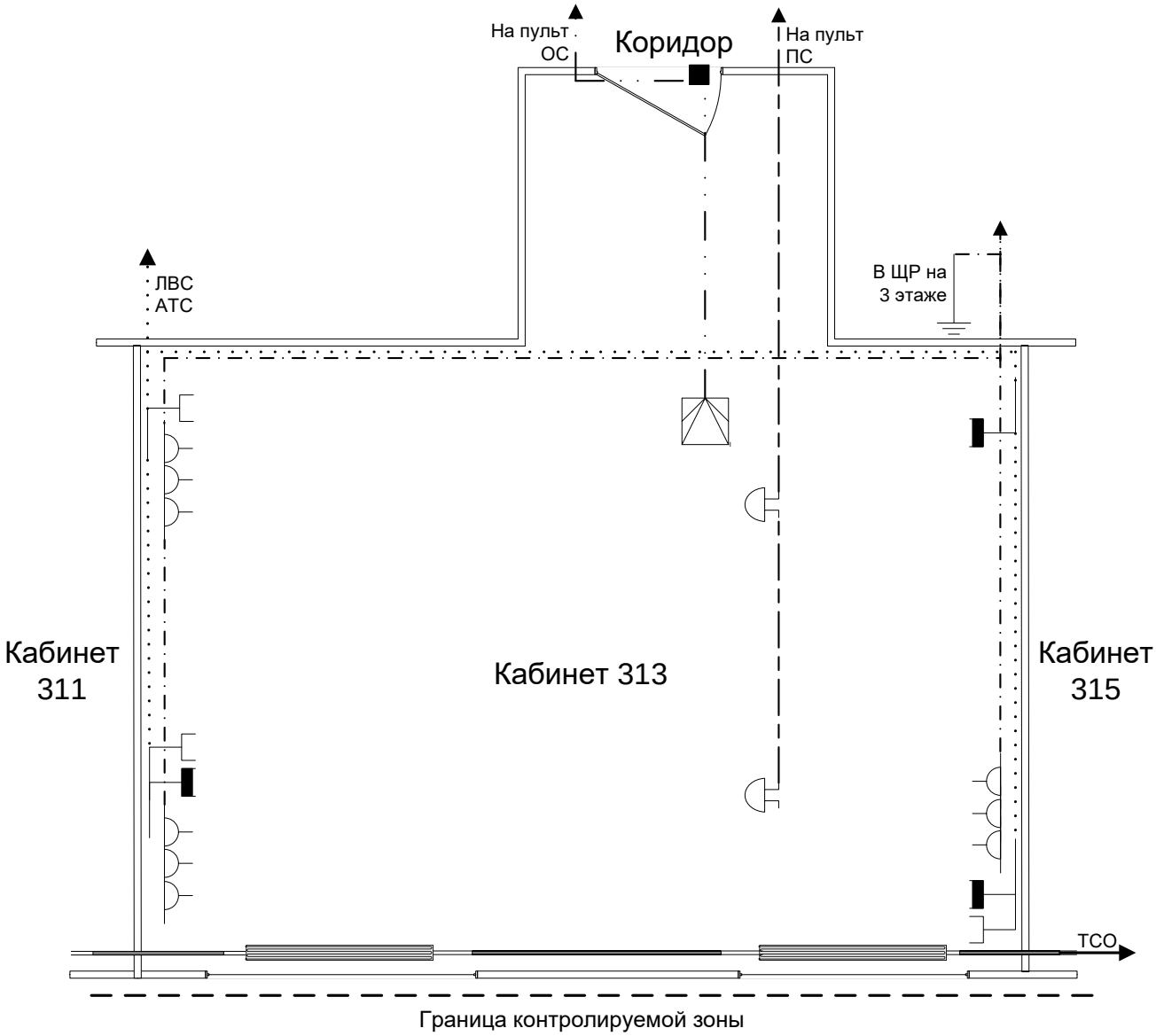
Линии пожарной сигнализации

Линии охранной сигнализации

Батарея отопления

Схема 11

Таможенное управление, кабинет № 313

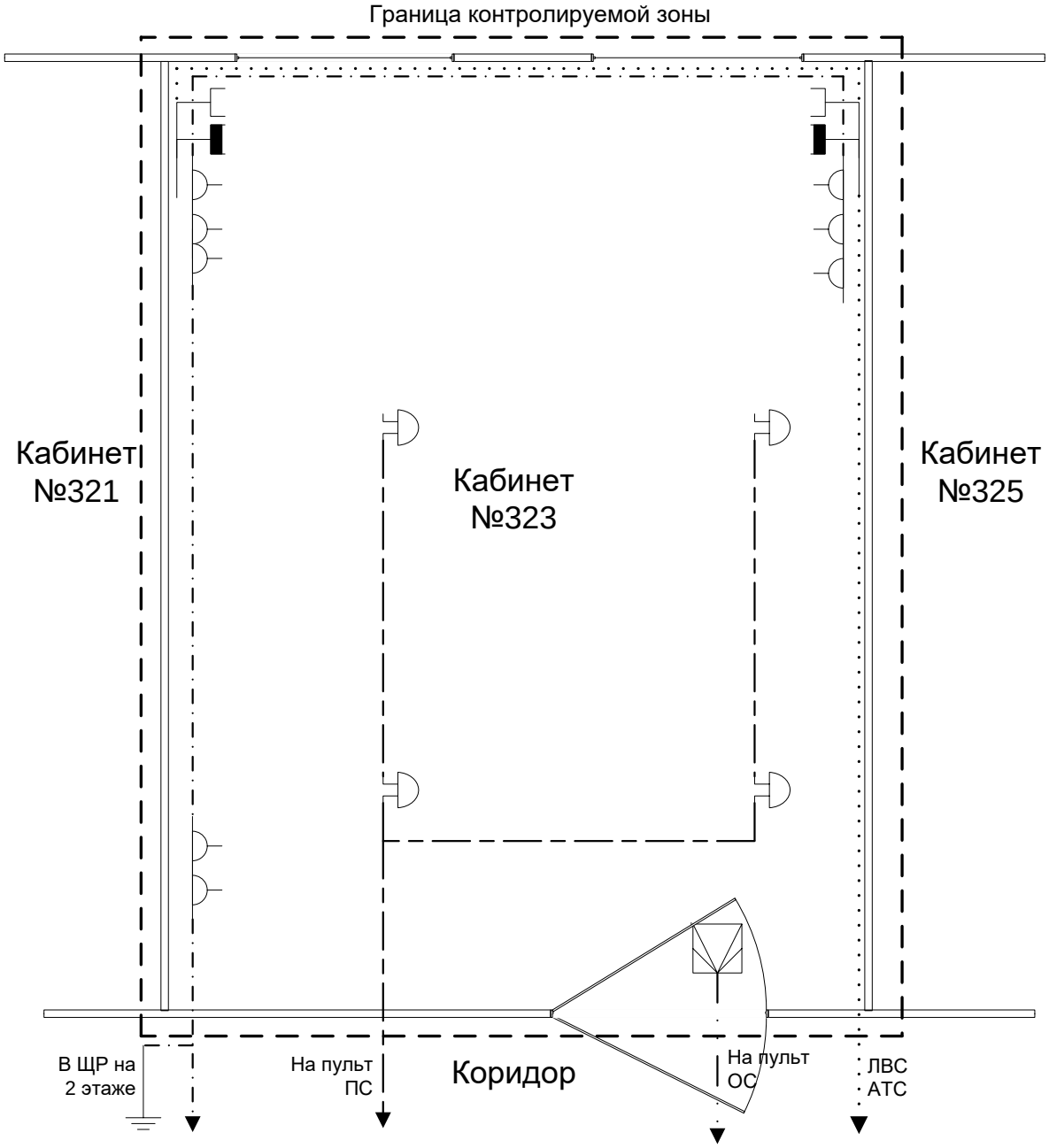


Условные обозначения:

- розетка ЛВС(сетевая)
- телефонная розетка
- извещатель охранный оптико-электронный
- розетка электропитания
- Извещатель пожарный
- Извещатель аккустический
- Извещатель охранный магнито-контактный
- Линии электропитания
- Телефонные линии и линии ЛВС
- Линии пожарной сигнализации
- Линии охранной сигнализации
- Батарея отопления
- Считыватель touch memory

Схема 12

Таможенное управление, кабинет № 323



Условные обозначения:

- розетка ЛВС(сетевая)
- телефонная розетка
- извещатель охранный оптико-электронный
- розетка электропитания
- Извещатель пожарный
- Извещатель аккустический
- Извещатель охранный магнито-контактный
- Линии электропитания
- Телефонные линии и линии ЛВС
- Линии пожарной сигнализации
- Линии охранной сигнализации
- Батарея отопления
- Считыватель touch memory

Продолжение приложения Е

Перечень средств защиты информации, установленных на АС

№ п/п	Наименование и тип технического средства	Заводской номер	Сведения о сертификате/№ лицензии	Место и дата установки
5.	СЗИ от НСД «Dallas-Lock 8.0-C»	10695-3286-259 3982084	Сертификат ФСТЭК России: № 2945 действителен до 16.08.2018 г.	ПЭВМ №1-ПЭВМ №6 15.10.17
6.	Средство антивирусной защиты Kaspersky Endpoint Security 10 для Windows	17E0-00045104 EEF4C3B /Л866418	Сертификат ФСТЭК России № 3025 (от 25.11.2013 до 25.11.2019).	ПЭВМ№1-ПЭВМ №6 06.11.17
7.	Персональное средство аутентификации (электронный ключ) eToken	470BF614	Сертификат ФСТЭК России: № 1883 действителен до 11.08.2019 г	-
		47066914		
		47064A14		
		47063814		
		46A1D814		
		46FBFE14		
		470BF714		
		470BF712		
8.	АПКШ "Континент IPC-100"	G2UGEP87 /E828180	Сертификат ФСТЭК № 3008 действителен до 01.11.2019 г	-
		JF873TGY /Г641540		
		V2K8DPRY /Г641515		
		SJ8818VT /Г641509		
		4Z2ME1ZE /Г641527		

2.5. Перечень используемых в АС программных средств

№ п/п	Наименование и тип программного средства	Описание	Примечание
1	Операционная система Microsoft Windows XP,7	Операционная система	-
2	WinRAR	Архиватор	-
3	Athena AES Drive	Драйвер считывателя	-

№ п/п	Наименование и тип программного средства	Описание	Примечание
		Athena	
4	eToken Runtime	Драйвер считывателя eToken	-
5	Free Commander	Файловый менеджер	-
6	Microsoft NetFramework 3.5	Программная платформа	-
7	Microsoft Office 2010	Офисный пакет	-
8	Агент администрирования Kaspersky	Агент для связи к северу администрирования Kaspersky	-
9	Аист-М	Автоматизированная информационная система	-

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

№ п./п.	Наименование документа	Инвентарный номер документа	Дата Регистрации Документа

4. Результаты периодического контроля

Дата проведения	Наименование организации, проводившей проверку	Результаты проверки, номер отчетного документа

5. Лист регистрации изменений

№	Дата измен.	Состав вносимых изменений	Документ, на котором отражены текущие изменения	Подпись руковод. ОВТ	Подпись органа по аттестации