МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Тульский государственный университет»

Институт прикладной математики и компьютерных наук

Кафедра информационной безопасности

**ОПИСАНИЕ ОБЪЕКТА ИНФОРМАТИЗАЦИИ**

Отчёт по практической работе

по курсу «Обеспечение доверия к информационной безопасности  
защищённых автоматизированных систем управления»

Выполнил: студент группы 230781 \_\_\_\_\_\_\_\_\_ Ивлев А.Р.

(подпись)

Проверил: руководитель \_\_\_\_\_\_\_\_\_ Куприянов А.О.

(подпись)

Тула 2022

**РЕФЕРАТ**

Практическая работа по теме «Обеспечение доверия к информационной безопасности».

Количество книг отчёта – 1, объём работы – 25 страниц, на которых размещены 2 рисунка и 8 таблиц, использовалось 12 источников.

**СОДЕРЖАНИЕ**

[ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ 5](#_Toc104507556)

[ВВЕДЕНИЕ 6](#_Toc104507557)

[1 Общие сведения об автоматизированной системе управления 7](#_Toc104507558)

[1.1 Наименование информационной системы 7](#_Toc104507559)

[1.2 Место расположения объекта вычислительной техники 7](#_Toc104507560)

[2 Нормативно-правовые и нормативно-технические документы, в соответствии с требованиями которых разрабатывается система 7](#_Toc104507561)

[2.1 Перечень нормативно-правовых и/или нормативно-технических документов с указанием их реквизитов 7](#_Toc104507562)

[2.2 Основные требования нормативно-правовых и/или нормативно-технических документов, предъявляемые проектируемой системе защиты информации 7](#_Toc104507563)

[2.3 Перечень документов, разрабатываемых на этапе формирования требований к автоматизированной системе 8](#_Toc104507564)

[3 Условия эксплуатации информационной системы 9](#_Toc104507565)

[3.1 Сведения об архитектуре информационной системы, включающие описание структуры и состава, структурную схему с указанием информационных связей между компонентами информационной системы и иными информационными системами, в том числе с сетью Интернет 9](#_Toc104507566)

[3.2 Описание технологического процесса обработки информации и режимы доступа к информационным ресурсам, включающее описание всех типов внешних, внутренних пользователей, полномочий пользователей и тип доступа к информационным ресурсам 11](#_Toc104507567)

[4 Состав информационной системы 13](#_Toc104507568)

[4.1 Состав программно-технических средств информационной системы 13](#_Toc104507569)

[4.2 Состав общесистемного и прикладного программного обеспечения информационной системы 13](#_Toc104507570)

[4.3 Состав телекоммуникационного оборудования информационной системы и используемые для передачи информации линии связи 14](#_Toc104507571)

[4.4 Состав средств защиты информации, используемых в информационной системе 14](#_Toc104507572)

[5 Техническое задание на разработку 15](#_Toc104507573)

[5.1 Систематизация требований к разрабатываемой системе защиты информации вашей автоматизированной/информационной системы 15](#_Toc104507574)

[5.2 Установление требований доверия к продукции, применяемой для защиты информации. Обоснование выбранных требований доверия 18](#_Toc104507575)

[6 Оценка процессов. Аттестация объектов информатизации 20](#_Toc104507576)

[6.1 Перечень документов, предоставляемых владельцем автоматизированной системы на аттестацию 20](#_Toc104507577)

[6.2 Перечень документов, разрабатываемых органом по аттестации по результатам аттестационных испытаний 21](#_Toc104507578)

[7 Оценка внешних условий. Лицензирование предприятий и организаций в области защиты информации 21](#_Toc104507579)

[7.1 Требования к организации, предоставляющей услуги по аттестации объекта информатизации 21](#_Toc104507580)

[7.2 Перечень требований и условий к соискателю лицензии по технической защите конфиденциальной информации 22](#_Toc104507581)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 24](#_Toc104507582)

# ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

АВЗ – Антивирусная защита;

АИС – Автоматизированная информационная система;

АРМ – Автоматизированное рабочее место;

ВТСС – Вспомогательные технические средства и системы;

ГОСТ – Межгосударственный стандарт;

ЗБ – Задание по безопасности;

ИСПДн – Информационная система персональных данных;

ОИ – Объект информатизации;

ОТСС – Основные технические средства и системы;

ОУД – Оценочный уровень доверия;

ПДн – Персональные данные;

ПК – Персональный компьютер;

ПО – Программное обеспечение;

ПП РФ – Постановление Правительства Российской Федерации;

СОВ – Средство обнаружения вторжений;

ФЗ – Федеральный закон;

ФСТЭК – Федеральная служба по техническому и экспортному контролю;

ФТБ – Функциональное требование безопасности.

# ВВЕДЕНИЕ

Для обеспечения нормального хода различных технологических и производственных процессов в системе необходимо обеспечить правильную работу не только функциональность системы, но и ее защиту для предотвращения нежелательного воздействия злоумышленников.

Необходимый уровень доверия к безопасности должен быть обеспечен на этапах разработки, проектирования, сопровождения и использования системы пользователями. Необходимо постоянно поддерживать актуальность данных о нарушениях информационной безопасности и векторов атак для совершенствования механизмов защиты и внедрения новых технологий безопасности.

Предметом исследования в данной практической работе является автоматизированная информационная система «Нотариальная контора».

Целью данной работы является закрепление, углубление и обобщение знаний, полученных при изучении курса «Обеспечение доверия к информационной безопасности защищенных автоматизированных систем управления»; развитие навыков применения теоретических положений при решении задач по специальности.

# 1 Общие сведения об автоматизированной системе управления

## 1.1 Наименование информационной системы

Автоматизированная информационная система «Нотариальная контора».

## 1.2 Место расположения объекта вычислительной техники

Тульская область, г. Суворов, ул.ХХХ, д.ХХХ, этаж 2, офис №10.

# 2 Нормативно-правовые и нормативно-технические **документы, в соответствии с требованиями которых разрабатывается система**

## 2.1 Перечень нормативно-правовых и/или нормативно-технических документов с указанием их реквизитов

1. ФЗ № 149 от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации»;
2. ФЗ № 152 от 26.07.2006 г. «О персональных данных»;
3. Приказ ФСТЭК № 21 от 18.02.2013 г. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
4. ПП РФ № 1119 от 01.11.2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

## 2.2 Основные требования нормативно-правовых и/или нормативно-технических документов, предъявляемые проектируемой системе защиты информации

Информация о клиентах организации конфиденциальна для лиц, не имеющих отношение к ее обработке, а также не должна распространяться без разрешения клиентов[1].

Клиент может в любой момент запросить хранимые о нем данные и потребовать их удалить. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных[2].

Каждый сотрудник перед началом работы обязан пройти идентификацию и аутентификацию. Права доступа сотрудников должны быть минимальны, но достаточны для корректной работы в системе. Сотрудники имеют право устанавливать и запускать только разрешенное к использованию в информационной системе ПО. На каждом персональном компьютере и сервере должна находиться АВЗ для обнаружения программ, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации[3].

Безопасность ПДн при их обработке в информационной системе обеспечивает оператор этой системы. Договор между оператором и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность персональных данных при их обработке в информационной системе[4].

## 2.3 Перечень документов, разрабатываемых на этапе формирования требований к автоматизированной системе

При формировании требований к автоматизированной системе необходимо разработать следующие документы[5][6][7]:

* «Разработка и утверждение технического задания на создание АСЗИ»;
* «Акт классификации автоматизированной системы»;
* «Технический паспорт на объект информатизации «Нотариальная контора»;
* «Перечень сведений конфиденциального характера информационной системы персональных данных»;
* «Перечень сотрудников, допущенных к обработке персональных данных»;
* «Модель угроз безопасности информации»;
* «Описание организации информационной базы»;
* «Описание систем классификации и кодирования»;
* «Описание массива информации»;
* «Описание информационного массива»;
* «Описание базы данных»;
* «Описание программного обеспечения».

# 3 Условия эксплуатации информационной системы

## 3.1 Сведения об архитектуре информационной системы, включающие описание структуры и состава, структурную схему с указанием информационных связей между компонентами информационной системы и иными информационными системами, в том числе с сетью Интернет

Рисунки 1 и 2 отображают размещение технических средств и расположение КЗ в здании.

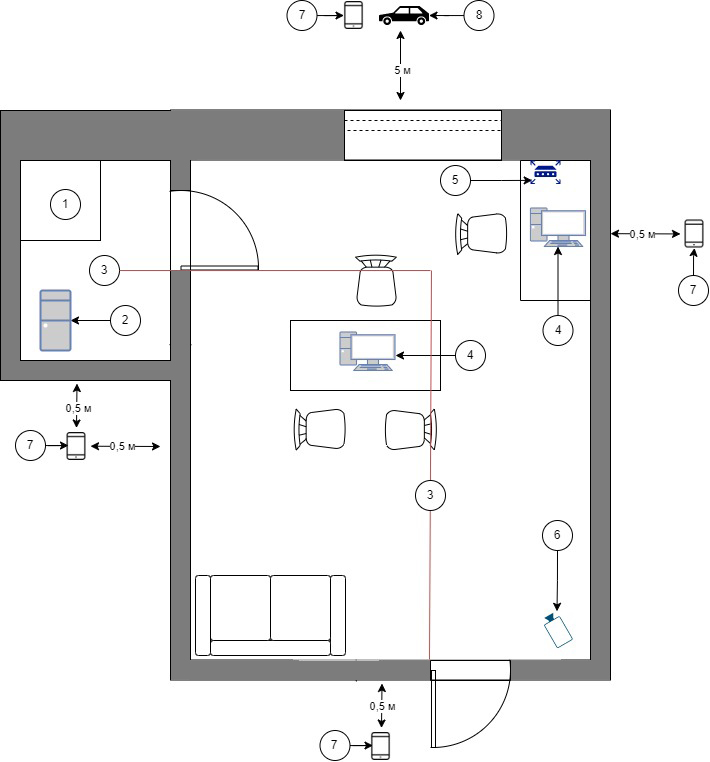


Рисунок 1 – План-схема размещения технических средств

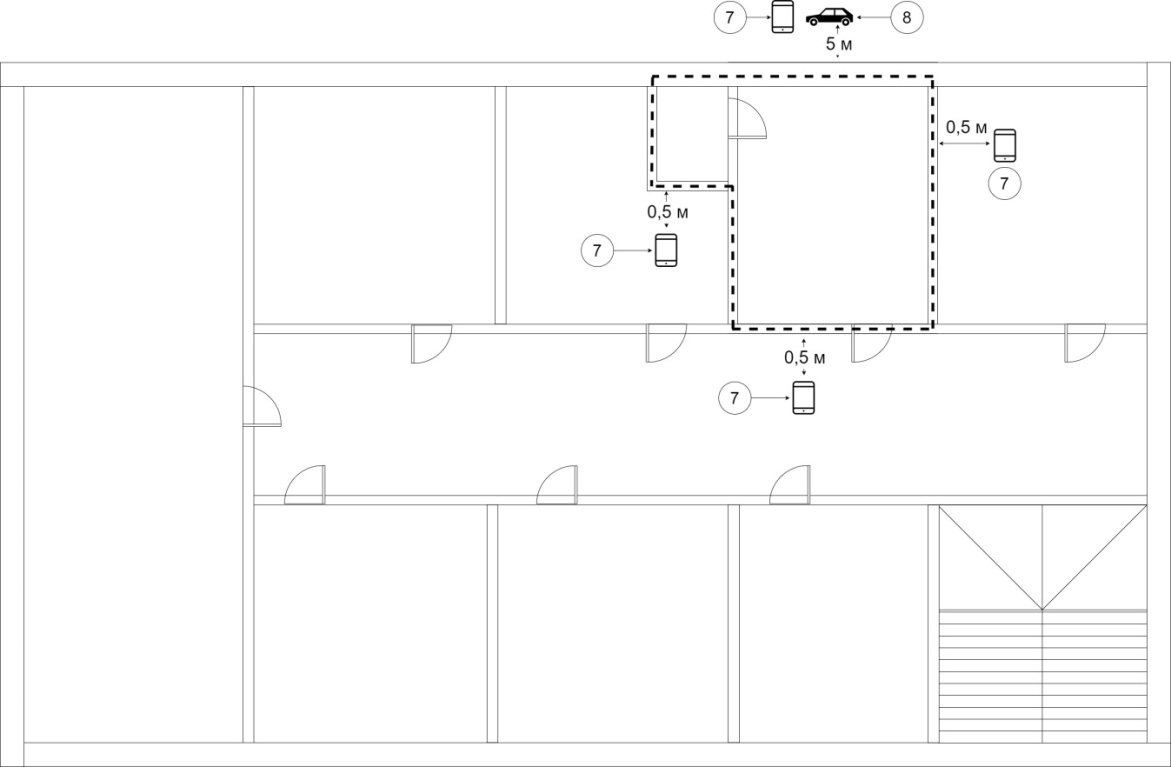


Рисунок 2 – План-схема расположения КЗ в здании (контролируемая зона выделена пунктиром)

Использованные обозначения:

1. Сейф, в котором хранятся штамп нотариуса, бланки, документы в печатном виде и иные физические носители информации;
2. Сервер;
3. Датчики пожарной безопасности, 2 шт., подключенные к общей системе пожарной безопасности здания;
4. АРМ, 2 шт;
5. Роутер;
6. Камера, получаемые данные с которой выходят за пределы контролируемой зоны;
7. Ближайшее место возможного размещения носимых средств разведки;
8. Ближайшее место возможного размещения возимых средств разведки.

Носимые средства разведки актуальны для объекта информатизации и могут быть размещены как на улице, так и в соседних офисах (расстояние от 0,5 метра). Возимые средства разведки актуальны и могут находиться только со стороны улицы (расстояние от 5 метров). Стационарные средства разведки неактуальны, поскольку в Туле нет иностранных посольств (территорий, принадлежащих другим государствам).

## 3.2 Описание технологического процесса обработки информации и режимы доступа к информационным ресурсам, включающее описание всех типов внешних, внутренних пользователей, полномочий пользователей и тип доступа к информационным ресурсам

По типу ИСПДн является локальной и имеющей подключение к сетям связи общего пользования. Организация системы клиент-серверная. Режим обработки ПДн многопользовательский. Система не имеет разграничения прав доступа. Все технические средства ИСПДн находятся в пределах Российской Федерации.

Объектами автоматизации являются процесс сбора, обработки, проверки целостности и выдачи биометрических данных.

AC выполняет следующие функции:

* Приём и запись ПДн на носители;
* Выдача ПДН в цифровом виде;
* Проверка целостности информации.

В таблице 1 указаны сотрудники, работающие с АИС «Нотариальная контора».

Таблица 1 – Перечень сотрудников

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| №  п/п | Ф.И.О. | Образование, учебное  заведение, специальность | Стаж работы | Должность |
|  | Ухххххххххххх  Сххххххххххх  Вххххххххххххх | Высшее. 1998г.  Тульский Государственный Университет.  Специальность: «Юриспруденция» | 20 лет | Нотариус |
|  | Бххххххх  Ахххххххххх  Аххххххххххх | Высшее. 2016г.  Институт Бизнеса, Права и информационных технологий.  Специальность: «Юриспруденция» | 5 лет | Помощник нотариуса |

Пользователи системы собирают ПДн клиентов на своих АРМ, после чего с помощью специализированного ПО отправляют данные на локальный сервер для их длительного хранения. При необходимости с помощью специализированного ПО пользователи системы могут быть удалить или запросить ПДн с сервера для их последующей обработки.

# 4 Состав информационной системы

## 4.1 Состав программно-технических средств информационной системы

В таблицах 2 и 3 указаны технические средства, находящиеся в АИС «Нотариальная контора».

Таблица 2 – Состав ОТСС объекта

|  |  |  |  |
| --- | --- | --- | --- |
| № пп | Тип ОТСС | Заводской номер | Примечание |
|  | Моноблок Lenovo IdeaCentre 520-24IKU | xxxxxx | Рабочее место нотариуса |
|  | Моноблок Lenovo IdeaCentre 520-24IKU | xxxxxx | Рабочее место помощника нотариуса |
|  | Принтер Canon MF211 | xxxxxx |
|  | Wi-Fi роутер D-Link DIR-615 | xxxxxx |
|  | Сервер Lenovo ThinkSystem ST50 | xxxxxx | Сервер |

Таблица 3 – Состав ВТСС объекта

|  |  |  |  |
| --- | --- | --- | --- |
| № пп | Тип ВТСС | Заводской номер | Примечание |
|  | Датчики пожарные | xxxxxx | 2 шт. |
|  | Беспроводная IP Wi-Fi видеокамера | xxxxxx |  |

## 4.2 Состав общесистемного и прикладного программного обеспечения информационной системы

В таблице 4 указан состав используемого ПО в системе.

Таблица 4 – Программное обеспечение ИС

|  |  |  |  |
| --- | --- | --- | --- |
| № пп | Наименование | Назначение | Примечание |
|  | Windows 10 Enterprise | Системное ПО | Рабочее место нотариуса |
|  | АРМ нотариуса «Табеллион» | Прикладное ПО |
|  | OpenSSL | Прикладное ПО |
|  | Secret Net Studio | Средство защиты от НСД,  антивирусная защита |
|  | Windows 10 Enterprise | Системное ПО | Рабочее место помощника нотариуса |
|  | АРМ нотариуса «Табеллион» | Прикладное ПО |
|  | OpenSSL | Прикладное ПО |
|  | Secret Net Studio | Средство защиты от НСД, антивирусная защита |
|  | Linux Ubuntu 21 | Системное ПО | Сервер |
|  | Secret Net LSP | Средство защиты от НСД,  антивирусная защита |
|  | OpenSSL | Прикладное ПО |
|  | Microsoft SQL Server 2016 | Прикладное ПО |

## 4.3 Состав телекоммуникационного оборудования информационной системы и используемые для передачи информации линии связи

В АИС находится роутер D-Link DIR-615, к которому дистанционно подключаются персональные компьютеры и сервер для организации локальной сети. Роутер подключен волоконно-оптической линией к сети Интернет.

## 4.4 Состав средств защиты информации, используемых в информационной системе

В таблице 5 указаны использующие в системе программные средства защиты информации.

Таблица 5 – Программные средства защиты информации

|  |  |  |
| --- | --- | --- |
| Наименование | Сведения о сертификате | Примечание |
| Secret Net Studio | Подтверждает соответствие требованиям руководящих документов по 2 уровню доверия, по 3 классу защищенности СВТ, 2 классу защиты МЭ тип "В" (ИТ.МЭ.В2.ПЗ). Может применяться в АС до классов 1Б, 2А, 3А включительно (РД АС, 1992 г.), АС до классов 3А, 3Б, 2А, 2Б включительно (приказ ФСТЭК России №025 от 20.10.2016), ИСПДн до УЗ1 включительно, ГИС до 1 класса включительно, АСУ ТП до 1 класса включительно, объектах КИИ до 1 категории значимости включительно | Рабочие места нотариуса и помощника нотариуса |
| Secret Net LSP | Соответствует требованиям руководящих документов по 5 классу защищенности СВТ, требованиям к межсетевым экранам типа «В» 4 класса защиты, требованиям к 4 уровню доверия средств обеспечения безопасности информационных технологий | Сервер |

# 5 Техническое задание на разработку

## 5.1 Систематизация требований к разрабатываемой системе защиты информации вашей автоматизированной/информационной системы

Таблица 6 содержит информацию о ПДн, обрабатываемых в системе[2].

Таблица 6 – Перечень персональных данных, обрабатываемых в АС

|  |  |  |  |
| --- | --- | --- | --- |
| № | ПДн | Перечень характеристик безопасности | Категории ПДн |
|  | ФИО | Конфиденциальность, целостность, доступность | Общедоступные |
|  | Паспортные данные | Иные |
|  | Сведения о семейном положении |
|  | Сведения о близких родственниках |
|  | Сведения о финансовом положении |

Для данной системы характерны следующие критерии:

* По форме отношений между организацией и субъектами происходит обработка персональных данных субъектов, не являющихся работниками организации;
* Для данной системы характерны угрозы 3-го типа, не связанные с наличием недекларированных возможностей в системном и прикладном ПО.

Для ИСПДн должен быть обеспечен 4 уровень защищенности[4].

* Организация режима обеспечения безопасности помещений, в которых размещена ИСПДн, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
* Обеспечение сохранности носителей персональных данных;
* Утверждение руководителем оператора персональных данных документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в ИСПДн, необходим для выполнения ими служебных (трудовых) обязанностей;
* 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.

Перечень мер по обеспечению безопасности персональных данных ИСП, обеспечивающих 4 уровень защищенности, представлен в таблице 7[3].

Таблица 7 – Перечень мер по обеспечению безопасности ПДн

|  |  |
| --- | --- |
| Условное обозначение и номер меры | Содержание мер по обеспечению безопасности персональных данных |
| 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 или компрометации средств аутентификации |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации |
| УПД.1 | Управление учетными записями 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 |
| УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств |
| *Продолжение таблицы 6* | |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций |
| 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.7 | Защита информации о событиях безопасности |
| АВЗ.1 | Реализация антивирусной защиты |
| АВЗ.2 | Обновление базы данных признаков вредоносных компьютерных программ |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации |
| 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 |
| ЗИС.3 | Обеспечение защиты персональных данных от раскрытия, модификации и навязывания при ее передаче по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи |

Для обеспечения 4-го уровня защищенности персональных данных при их обработке в ИСПДн применяются сертифицированные по требованиям безопасности информации средства защиты информации 6 класса[3]:

* Средства антивирусной защиты 6 класса (ИТ.САВЗ.А6.ПЗ, ИТ.САВЗ.Б6.ПЗ, ИТ.САВЗ.В6.ПЗ, ИТ.САВЗ.Г6.ПЗ);
* Межсетевой экран 6 класса (ИТ.МЭ.А6.ПЗ, ИТ.МЭ.Б6.ПЗ, ИТ.МЭ.В6.ПЗ, ИТ.МЭ.Г6.ПЗ, ИТ.МЭ.Д6.ПЗ);
* Средства вычислительной техники 6 класса;
* Системы обнаружения вторжений 6 класса (ИТ.СОВ.С6.ПЗ, ИТ.СОВ.У6.ПЗ);
* Операционная система 6 класса (ИТ.ОС.А6.ПЗ);
* Средства контроля съемных машинных носителей информации 6 класса (ИТ.СКН.П6.ПЗ);
* Средства доверенной загрузки 6 класса (ИТ.СДЗ.ЗЗ6.ПЗ).

## 5.2 **Установление требований доверия к продукции, применяемой для защиты и**нформации. Обоснование выбранных требований доверия

Т.к. обеспечение безопасности происходит для разработанной ранее системы, то ИСПДн имеет оценочный уровень доверия 2 (ОУД2) [8].

ОУД2 обеспечивает доверие посредством ЗБ с полным содержанием и посредством анализа выполнения ФТБ из данного ЗБ с использованием функциональной спецификации, спецификации интерфейсов, руководств, а также базового описания архитектуры для понимания режима безопасности.

В таблице 8 содержится классы и компоненты доверия ОУД2.

Таблица 8 – Оценочный уровень доверия 2

|  |  |
| --- | --- |
| Класс доверия | Компоненты доверия |
| ADV: Разработка | ADV\_ARC.1 Описание архитектуры безопасности |
| ADV\_FSP.2 Детализация вопросов безопасности в функциональной спецификации |
| ADV\_TDS.1 Базовый проект |
| AGD: Руководства | AGD\_OPE.1 Руководство пользователя по эксплуатации |
| AGD\_PRE.1 Подготовительные процедуры |
| ALC: Поддержка жизненного цикла | ALC\_CMC.2 Использование системы УК |
| ALC\_CMS.2 Охват УК частей ОО |
| ALC\_DEL.1 Процедуры поставки |
| ASE: Оценка задания по безопасности | ASE\_CCL.1 Утверждения о соответствии |
| ASE\_ECD.1 Определение расширенных компонентов |
| ASE\_INT.1 Введение ЗБ |
| ASE\_OBJ.2 Цели безопасности |
| ASE\_REQ.2 Производные требования безопасности |
| ASE\_SPD.1 Определение проблемы безопасности |
| ASE\_TSS.1 Краткая спецификация ОО |
| ATE: Тестирование | ATE\_COV.1 Свидетельство покрытия |
| ATE\_FUN.1 Функциональное тестирование |
| ATE\_IND.2 Выборочное независимое тестирование |
| AVA: Оценка уязвимостей | AVA\_VAN.2 Анализ уязвимостей |

Т.к. к системе должны быть применены средства защиты 6 уровня доверия, необходимо, чтобы используемые средства соответствовали следующим требованиям[9]:

1. Требования к разработке и производству средства:
   1. Требования к проектированию архитектуры безопасности средства;
   2. Требования к разработке функциональной спецификации средства;
   3. Требования к проектированию средства;
   4. Требования к разработке проектной (программной) документации;
   5. Требования к средствам разработки, применяемым для создания средства;
   6. Требования к управлению конфигурацией средства;
   7. Требования к разработке документации по безопасной разработке средства;
   8. Требования к разработке эксплуатационной документации;
2. Требования к проведению испытаний средства:
   1. Требования к тестированию средства;
   2. Требования к испытаниям по выявлению уязвимостей и недекларированных возможностей средства;
3. Требования к поддержке безопасности средства:
   1. Требования к устранению недостатков средства;
   2. Требования к обновлению средства;
   3. Требования к документированию процедур устранения недостатков и обновления средства;
   4. Требования к информированию об окончании производства и (или) поддержки безопасности средства.

Список средств защиты с соответствующими им уровнями доверия представлен в таблице 9.

Таблица 9 – Уровни доверия к средствам защиты системы

|  |  |  |
| --- | --- | --- |
| № | Наименование СЗИ | Соответствие требованиям |
| 1 | Secret Net Studio | Требования доверия(4), Требования к МЭ, Профиль защиты МЭ(В четвертого класса защиты. ИТ.МЭ.В4.ПЗ), Требования к САВЗ, Профиль защиты САВЗ(А четвертого класса защиты. ИТ.САВЗ.А4.ПЗ), Профиль защиты САВЗ(Б четвертого класса защиты. ИТ.САВЗ.Б4.ПЗ), Профиль защиты САВЗ(В четвертого класса защиты. ИТ.САВЗ.В4.ПЗ), Профиль защиты САВЗ(Г четвертого класса защиты. ИТ.САВЗ.Г4.ПЗ), Требования к СКН, Профиль защиты СКН(контроля подключения съемных машинных носителей информации четвертого класса защиты. ИТ.СКН.П4.ПЗ), Требования к СОВ, Профили защиты СОВ(узла четвертого класса защиты. ИТ.СОВ.У4.ПЗ), ЗБ, РД СВТ(5) |
| 2 | Secret Net LSP | Требования доверия(4), Требования к МЭ, Профиль защиты МЭ(В четвертого класса защиты. ИТ.МЭ.В4.ПЗ), РД СВТ(5) |

# 6 Оценка процессов. Аттестация объектов информатизации

## 6.1 Перечень документов, предоставляемых владельцем автоматизированной системы на аттестацию

Аттестация рассматриваемой системы не является обязательной и может быть проведена по инициативе самого заказчика. Для проведения работ по аттестации владелец объекта информатизации представляет в орган по аттестации следующие документы или их копии[10]:

1. «Технический паспорт на объект информатизации «Нотариальная контора»;
2. «Акт классификации информационной системы»;
3. «Модель угроз безопасности информации»;
4. «Техническое задание на создание ОИ «Нотариальная контора»;
5. «Проектная документация на систему защиты информации ОИ «Нотариальная контора»;
6. «Применяемые средства защиты информации для ОИ «Нотариальная контора»;
7. «Защита информации в ходе эксплуатации ОИ «Нотариальная контора»;
8. «Анализ уязвимостей ОИ «Нотариальная контора».

6**.2 Перечень документов, разрабатываемых органом по аттестации по результатам аттестационных испытаний**

Орган по аттестации разрабатывает следующие документы[10]:

1. «Программа аттестационных испытаний ОИ «Нотариальная контора»;
2. «Заключение по результатам аттестационных испытаний ОИ «Нотариальная контора»;
3. «Протокол аттестационных испытаний ОИ «Нотариальная контора»;
4. «Аттестат соответствия требованиям по защите информации на ОИ «Нотариальная контора».

# 7 Оценка внешних условий. Лицензирование предприятий и организаций в области защиты информации

## 7**.1 Требования к организации, предоставляющей услуги по аттестации объекта информатизации**

Лицензионными требованиями, предъявляемыми к лицензиату при осуществлении лицензируемого вида деятельности, являются[11]:

1. выполнение работ и оказание услуг лицензиатом;
2. повышение квалификации по лицензируемому виду деятельности причастных лиц не реже одного раза в 5 лет;
3. наличие помещений, в которых созданы необходимые условия для размещения работников, обсуждения информации ограниченного доступа и размещено производственное и испытательное оборудование, необходимое для осуществления лицензируемого вида деятельности;
4. использование принадлежащего лицензиату оборудования, необходимого для выполнения работ и оказания услуг:
5. поверенных измерительных приборов;
6. программно-технических средств, сертифицированных по требованиям безопасности информации;
7. использование автоматизированных систем, предназначенных для обработки конфиденциальной информации, а также средств защиты такой информации;
8. наличие технической и технологической документации, национальных стандартов и методических документов, необходимых для выполнения работ и оказания услуг.

## 7.**2 Перечень требований и условий к соискателю лицензии по технической защите конфиденциальной информации**

В качестве лицензирующего органа выступает Федеральная служба по техническому и экспортному контролю, поэтому лицензионными требованиями являются[12]:

1. наличие в штате по основному месту работы в соответствии со штатным расписанием следующего квалифицированного персонала:

* руководитель или уполномоченное руководить работами по лицензируемому виду деятельности лицо, имеющие высшее образование по направлению подготовки в области информационной безопасности и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 5 лет;
* инженерно-технические работники (не менее 2 человек), имеющие высшее образование по направлению подготовки в области информационной безопасности и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 3 лет;

1. наличие помещений, принадлежащих соискателю лицензии на праве собственности или ином законном основании, в которых созданы необходимые условия для размещения работников, производственного и испытательного оборудования, необходимого для осуществления лицензируемого вида деятельности, обсуждения информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну;
2. наличие оборудования, необходимого для выполнения работ и оказания услуг:

* производственного и испытательного оборудования;
* измерительных приборов, прошедших в установленном законодательством Российской Федерации порядке метрологическую поверку;
* программных средств, включая средства контроля эффективности защиты информации, сертифицированных по требованиям безопасности информации, а также средств контроля исходных текстов программного обеспечения;

1. наличие технической и технологической документации, национальных стандартов и методических документов, необходимых для выполнения работ и оказания услуг. Документы, содержащие информацию ограниченного доступа, должны быть получены в установленном законодательством Российской Федерации порядке;
2. наличие системы производственного контроля, включающей правила и процедуры проверки и оценки системы разработки средств защиты конфиденциальной информации, учета изменений, вносимых в проектную и конструкторскую документацию на разрабатываемую продукцию;
3. наличие системы производственного контроля, включающей правила и процедуры проверки и оценки системы производства средств защиты конфиденциальной информации, оценки качества выпускаемой продукции и неизменности установленных параметров, учета изменений, вносимых в техническую и конструкторскую документацию на производимую продукцию, учета готовой продукции.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ФЗ № 149 от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации»;
2. ФЗ № 152 от 26.07.2006 г. «О персональных данных»;
3. Приказ ФСТЭК № 21 от 18.02.2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
4. ПП РФ № 1119 от 01.11.2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
5. ГОСТ Р 51583-2014 «Порядок создания автоматизированных систем в защищенном исполнении»;
6. ГОСТ 34.201-2020 «Информационные технологии (ИТ). Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»;
7. ГОСТ 34.602-2020 «Информационные технологии (ИТ). Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;
8. ГОСТ Р ИСО/МЭК 15408-3-2013 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности»;
9. Приказ ФСТЭК № 76 от 02.06.2020 г. «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий»;
10. Приказ ФСТЭК № 77 от 29.04.2021 г. «Об утверждения порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»;
11. ПП РФ №79 от 03.02.2012 «О лицензировании деятельности по технической защите конфиденциальной информации»;
12. ПП РФ № 171 03.03.2012 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации».