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: лектор \_\_\_\_\_\_\_\_\_ Куприянов А.О.

(подпись)

Тула 2022

Оглавление

[1. Общие сведения об автоматизированной системе управления 3](#_Toc99070174)

[1.1. Объект ВТ 3](#_Toc99070175)

[1.2. Место расположения объекта вычислительной техники 3](#_Toc99070176)

[2.1. Перечень нормативно-правовых и/или нормативно-технических документов с указанием их реквизитов. 3](#_Toc99070177)

[2.2. Основные требования нормативно-правовых и/или нормативно-технических документов, предъявляемые проектируемой системе защиты информации. 3](#_Toc99070178)

[2.3. Перечень документов, разрабатываемых на этапе формирования требований к автоматизированной (информационной) системе. 4](#_Toc99070179)

[3. Условия эксплуатации информационной системы 5](#_Toc99070180)

[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. 5](#_Toc99070181)

[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. 7](#_Toc99070182)

[4. Состав информационной системы 8](#_Toc99070183)

[5. Техническое задание на разработку 9](#_Toc99070184)

[5.1. Систематизация требований к разрабатываемой системе защиты информации вашей автоматизированной/информационной системы 9](#_Toc99070185)

# 1. Общие сведения об автоматизированной системе управления

## 1.1. Объект ВТ

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/или 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. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ.
2. Федеральный закон «О персональных данных» от 26 июля 2006 г. № 152-ФЗ.
3. Постановление Правительства РФ от 01.11.2012 № 1119 "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.

1. № 149-ФЗ: в соответствии с федеральным законом информация, предоставленная клиентами салону, не должна распространяться, если подобные условия не оговорены с субъектом информации, а также должна быть конфиденциальна для лиц, не имеющих отношение к обработке данной информации. Информация о клиентах должна быть защищена от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации.
2. № 152-ФЗ: общедоступные данные предоставляются клиентом самостоятельно в момент записи в салон, при этом согласие на обработку персональных данных не подписывается. Следует уточнить, что собранные данные о клиенте могут быть ему предоставлены, а также удалены из системы по его требованию. Сотрудник, ответственный за обработку данных, должен соблюдать организационные меры по предотвращению неправомерного доступа к информации.
3. Постановление правительства № 1119: система защиты персональных данных должна включать организационные и технические меры, определенные с учетом актуальных угроз безопасности этих данных.

## 2.3. Перечень документов, разрабатываемых на этапе формирования требований к автоматизированной (информационной) системе.

1. ГОСТ 34.201-2020 Информационные технологии (ИТ). Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем
2. ГОСТ 34.602-2020 Информационные технологии (ИТ). Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы

# 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.

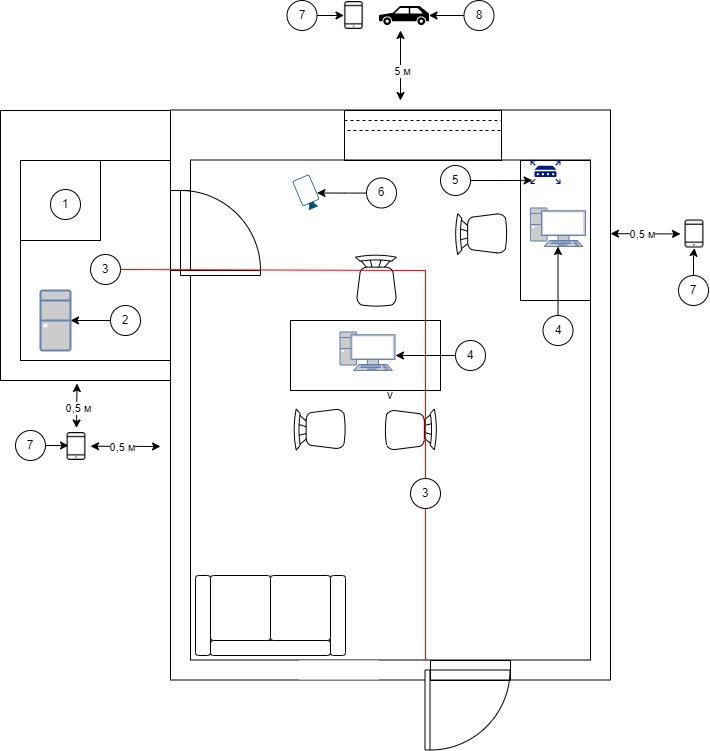


Рисунок 1 – План-схема офиса нотариальной конторы

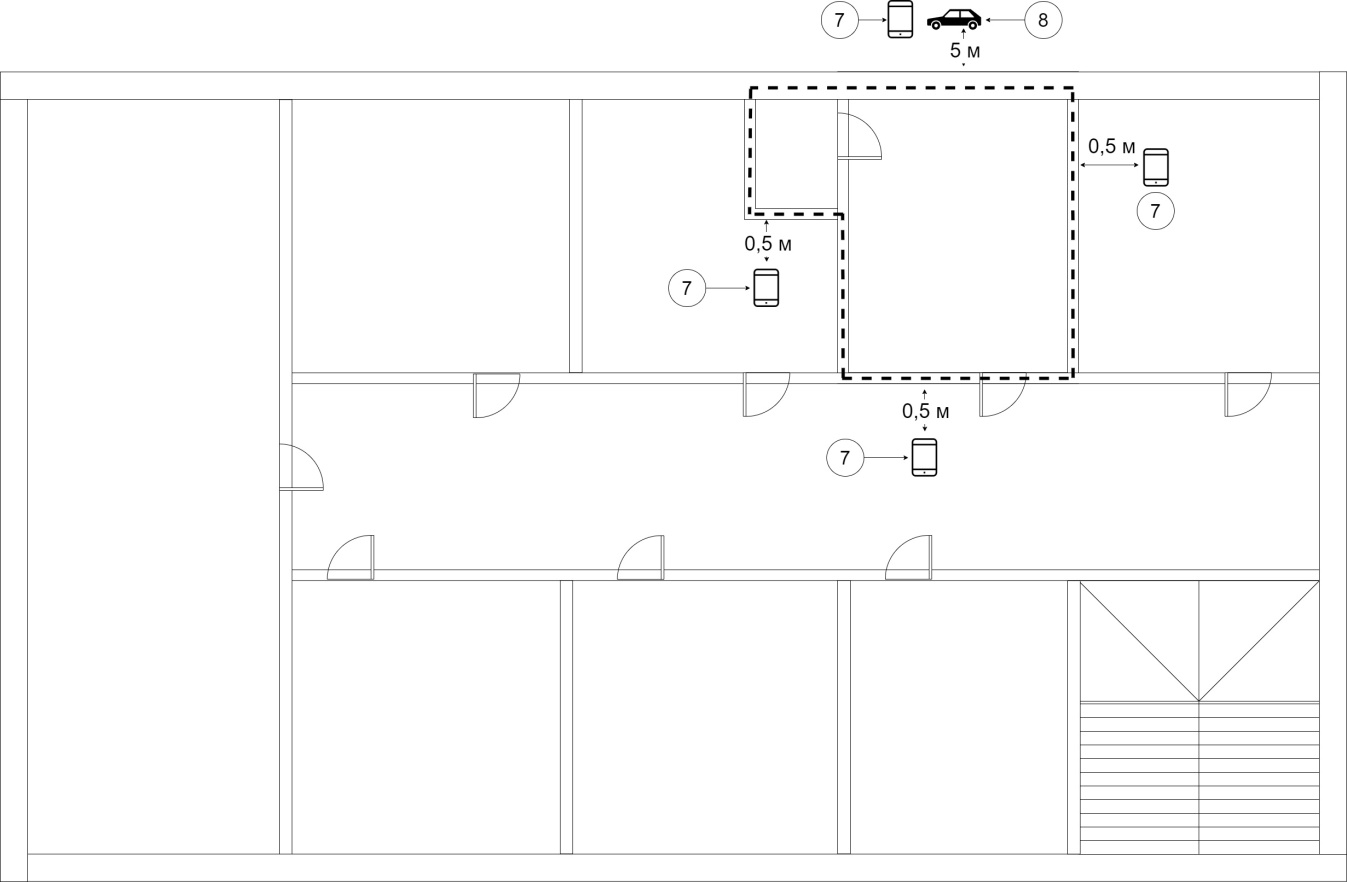


Рисунок 2 – План-схема (КЗ выделена пунктиром)

1. Сейф
2. Сервер
3. Датчики пожарной безопасности, 2 шт.
4. АРМ, 2 шт.
5. Роутер
6. Камера
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.

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

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 |

Тип: локальная ИСПДн, имеющая подключение к сетям связи общего пользования.

Организация системы: клиент-серверная.

Режим обработки ПДн: многопользовательский.

Режим разграничения прав доступа: система без разграничения прав доступа.

Местонахождение технических средств: система, все технические средства которой находятся в пределах Российской Федерации.

# 4. Состав информационной системы

Таблица №2. Состав ОТСС объекта

|  |  |  |  |
| --- | --- | --- | --- |
| **№ пп** | **Тип ОТСС** | **Заводской номер** | **Примечание** |
|  | Моноблок Lenovo IdeaCentre 520-24IKU | xxxxxx | Рабочее место нотариуса |
|  | Клавиатура Logitech | xxxxxx |
|  | Мышь Microsoft | xxxxxx |
|  | Моноблок Lenovo IdeaCentre 520-24IKU | xxxxxx | Раб очее место помощника нотариуса |
|  | Клавиатура Logitech | xxxxxx |
|  | Мышь Microsoft | xxxxxx |
|  | Принтер Canon MF211 | xxxxxx |
|  | Роутер 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 |  |
|  | Беспроводная IP Wi-Fi видеокамера | xxxxxx |  |

Таблица №4. Программные обеспечение ИС

|  |  |  |  |
| --- | --- | --- | --- |
| **№ пп** | **Наименование** | **Назначение** | **Примечание** |
|  | Windows 10 Enterprise | Системное ПО | Рабочее место нотариуса |
|  | Kaspersky Internet Security | Антивирусная защита |
|  | АРМ нотариуса "Экспресс" | Прикладное ПО |
|  | OpenSSL | Прикладное ПО |
|  | Secret Net Studio | Средство защиты от НСД |
|  | Windows 10 Enterprise | Системное ПО | Рабочее место нотариуса |
|  | Kaspersky Internet Security | Антивирусная защита |
|  | АРМ нотариуса "Экспресс" | Прикладное ПО |
|  | OpenSSL | Прикладное ПО |
|  | Secret Net Studio | Средство защиты от НСД |
|  | Linux Ubuntu 21 | Системное ПО | Сервер |
|  | Secret Net Studio | Средство защиты от НСД |
|  | OpenSSL | Прикладное ПО |
|  | MySQL | Прикладное ПО |

# 5. Техническое задание на разработку

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

Таблица №5. 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 |

Система имеет низкий уровень значимости (УЗ 3), т.к. для всех свойств безопасности информации определены низкие степени ущерба.

Информационная система имеет объектовый масштаб, т.к. она функционирует на объектах одного федерального органа государственной власти, органа государственной власти субъекта Российской Федерации, муниципального образования и (или) организации и не имеет сегментов в территориальных органах, представительствах, филиалах, подведомственных и иных организациях.

Согласно приказу ФСТЭК России от 15.02.2017 № 27, информационная система имеет уровень защищенности К3.

По форме отношений между организацией и субъектами происходит обработка персональных данных субъектов, не являющихся работниками организации.

Для данной системы характерны угрозы 3-го типа, т.к. для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

По количеству субъектов: менее 100 000 субъектов.

Для системы должен быть обеспечен уровень защищенности 4.

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;
2. обеспечение сохранности носителей персональных данных;
3. утверждение руководителем оператора [документа, определяющего перечень лиц](https://data-sec.ru/services/personal-data/documents/), доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
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.