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: \_\_\_\_\_\_\_\_\_ Куприянов А.О.

(подпись)

Тула 2022

**СОДЕРЖАНИЕ**

[1. Общие сведения об автоматизированной системе управления 3](#_Toc99562148)

[1.1. Объект ВТ 3](#_Toc99562149)

[1.2. Место расположения объекта вычислительной техники 3](#_Toc99562150)

[2. Нормативно-правовые и/или нормативно-технические документы, в соответствии с требованиями которых разрабатывается система 3](#_Toc99562151)

[2.1. Перечень нормативно-правовых и/или нормативно-технических документов с указанием их реквизитов. 3](#_Toc99562152)

[2.2. Основные требования нормативно-правовых и/или нормативно-технических документов, предъявляемые проектируемой системе защиты информации. 3](#_Toc99562153)

[2.3. Перечень документов, разрабатываемых на этапе формирования требований к автоматизированной системе. 4](#_Toc99562154)

[3. Условия эксплуатации информационной системы 5](#_Toc99562155)

[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](#_Toc99562156)

[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](#_Toc99562157)

[4. Состав информационной системы 8](#_Toc99562158)

[5. Техническое задание на разработку 9](#_Toc99562159)

[5.1. Систематизация требований к разрабатываемой системе защиты информации вашей автоматизированной/информационной системы 9](#_Toc99562160)

[5.2. Установление требований доверия к продукции, применяемой для защиты информации. Обоснование выбранных требований доверия. 12](#_Toc99562161)

# 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
2. Федеральный закон «О персональных данных» от 26.07.2006 г. № 152
3. Постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 г. № 1119
4. Приказ ФСТЭК 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»

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

Следующие нормативно-правовые и нормативно-технические документы определяют основные требования, предъявляемые проектируемой системе защиты информации:

1. ФЗ № 149 от 27.07.2006 г.
2. ФЗ № 152 от 26.07.2006 г.
3. ПП № 1119 от 01.11.2012 г.

ПДн не должны распространяться среди лиц, не имеющих отношение к обработке данных. Общедоступные данные предоставляются клиентом самостоятельно и могут быть ему предоставлены, а также удалены из системы по его требованию. Система защиты персональных данных должна включать организационные и технические меры для обеспечения безопасности этих данных.

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

Следующие ГОСТы регламентируют перечень документов, разрабатываемых на этапе формирования требований к автоматизированной системе:

ГОСТ Р 51583-2014

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

При формировании требований к автоматизированной системе необходимо разработать следующие документы:

* Описание организации информационной базы (П6)
* Описание систем классификации и кодирования (П7)
* Описание массива информации (П8)
* Описание информационного массива (В6)
* Описание базы данных (В7)
* Описание программного обеспечения (ПА)
* Техническое задание на создание автоматизированной системы (ТЗ)

# 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.

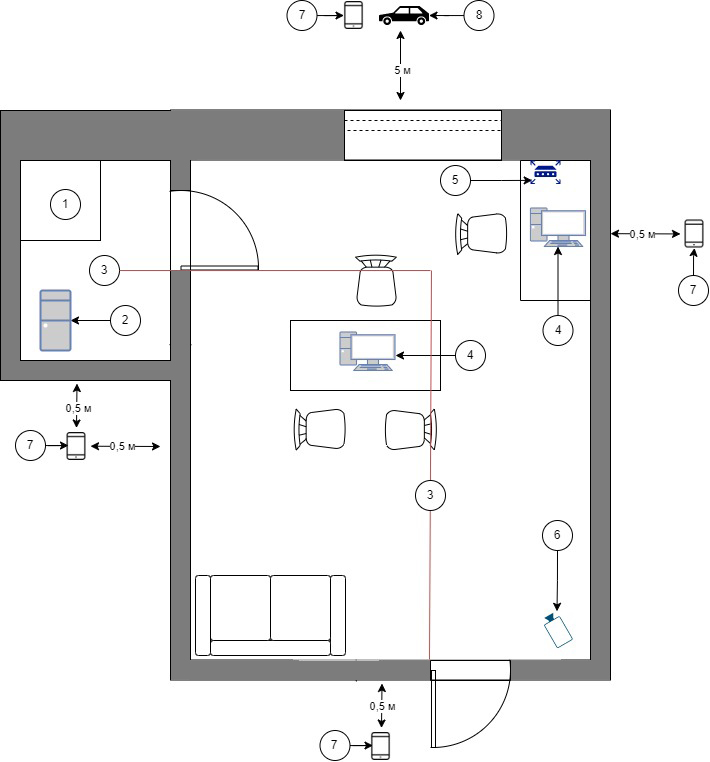


Рисунок 1 – План-схема размещения технических средств

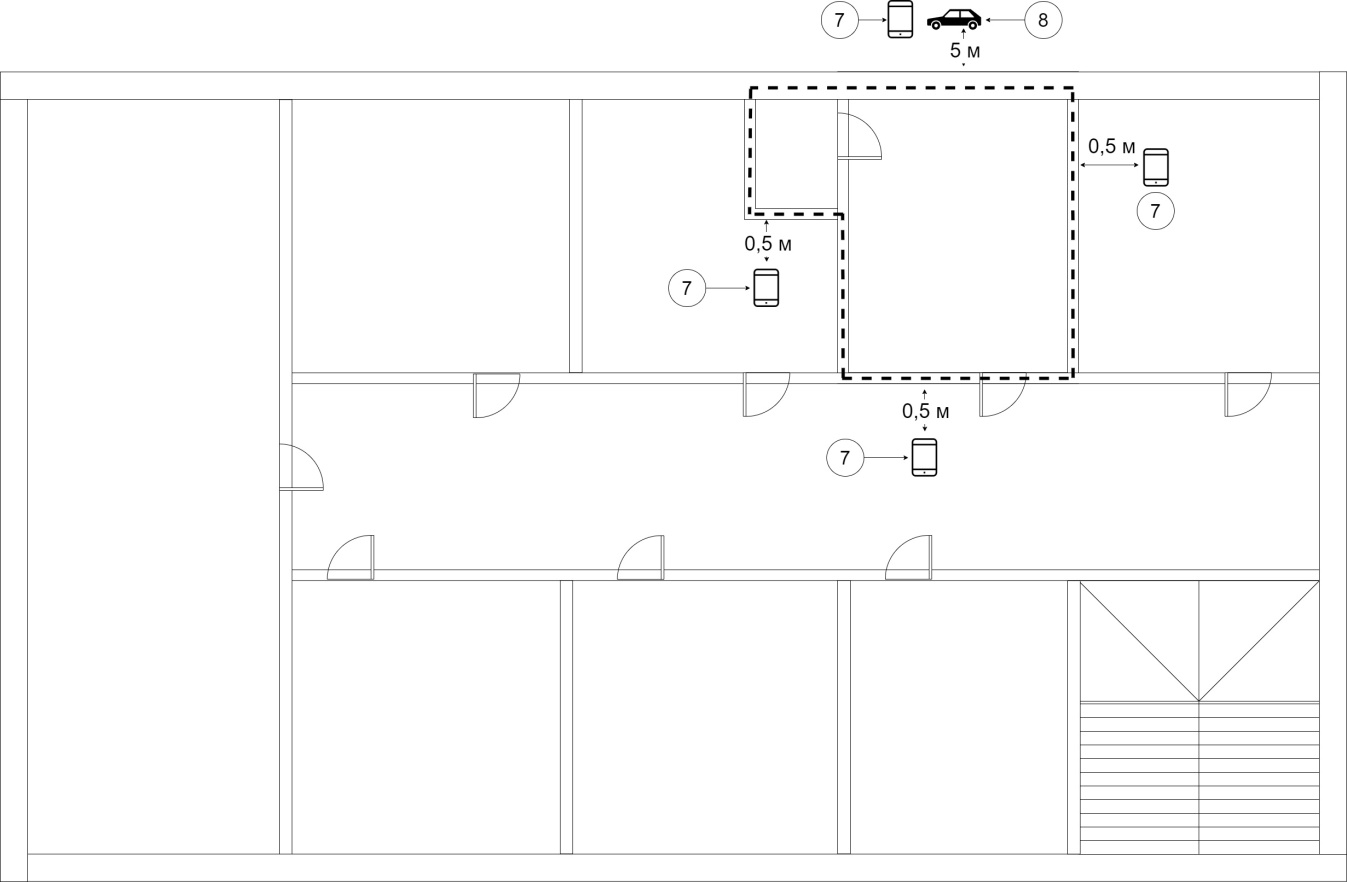


Рисунок 2 – План-схема (контролируемая зона выделена пунктиром)

1. Сейф

В сейфе хранятся штамп нотариуса, бланки, документы в печатном виде и иные физические носители информации.

1. Сервер
2. Датчики пожарной безопасности, 2 шт.

Датчики подключены к общей системе пожарной безопасности здания.

1. АРМ, 2 шт.
2. Роутер
3. Камера

Данные, получаемые с камеры, выходят за пределы контролируемой зоны.

1. Ближайшее место возможного размещения носимых средств разведки
2. 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 |

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.

# 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 | Рабочее 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 – 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 |
|  | 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 |

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.

* 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 ниже.

Таблица 6 – 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 |
| УПД.16 | | Управление взаимодействием с информационными системами сторонних организаций |
| РСБ.1 | | Определение событий безопасности, подлежащих регистрации, и сроков их хранения |
| *Продолжение таблицы 6* | | |
| 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:

* 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 информации. Обоснование выбранных требований доверия.

Т.к. обеспечение безопасности происходит для разработанной ранее системы, то, согласно ГОСТ Р ИСО/МЭК 15408-3-2013, ИСПДн имеет оценочный уровень доверия 2 (ОУД2).

ОУД2 обеспечивает доверие посредством заданий по безопасности (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.

Таблица 7 – 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:

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 8.

Таблица 8 – 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) |