

**ПОДСИСТЕМА УПРАВЛЕНИЯ ТРЕБОВАНИЯМИ**  
**МОДЕЛЬ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Версия 1.0

**СОГЛАСОВАНО**

Должность

Х.

Х. XXXX

(личная подпись)  
(расшифровка подписи)

«\_\_» \_\_\_\_\_ 2021 г

**Представители организации**  
**Разработчика**

Должность

Х.

Х. XXXX

(личная подпись)  
(расшифровка подписи)

«\_\_» \_\_\_\_\_ 2021 г

2021

КАФЕДРА КОМПЬЮТЕРНЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ (№ 12)

**ПРОЕКТИРОВАНИЕ ПОДСИСТЕМЫ УПРАВЛЕНИЯ  
ТРЕБОВАНИЯМИ**

**МОДЕЛЬ УГРОЗ И НАРУШИТЕЛЕЙ  
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Листов 23

Версия 1.0

Москва, 2021

## Аннотация

В документе «Модель угроз информационной безопасности» определены необходимые меры и средства по предотвращению реализации нарушителем угроз информационной безопасности в отношении ресурсов подсистемы «*Управление требованиями*». (ПУТР)

Модель угроз информационной безопасности является основой для определения состава необходимых режимных, организационно-технических и технических мер защиты ПУТР.

Модель угроз информационной безопасности ПУТР содержит:

- описание ПУТР;
- описание модели нарушителя информационной безопасности ПУТР;
- перечень угроз информационной безопасности (с привязкой к потенциальным нарушителям) ПУТР;
- меры по противодействию угрозам информационной безопасности в ПУТР.

## Содержание

|   |    |
|---|----|
| Термины и определения .....   | 7  |
| 1. Общие положения.....   | 9  |
| 1.1. Цели создания модели угроз и модели нарушителя информационной безопасности ..... | 9  |
| 1.2. Область применения .....   | 9  |
| 1.3. Общие принципы формирования .....  | 9  |
| 1.4. Правила пересмотра .....   | 9  |
| 2. Описание ПУТР .....  | 10 |
| 2.1. Наименование информационной системы .....  | 10 |
| 2.2. Цели создания и назначение ПУТР .....  | 10 |
| 2.3. Общее описание архитектуры ПУТР .....  | 10 |
| 2.4. Физические лица, имеющие доступ к компонентам ПУТР .....                         | 11 |
| 2.5. Информация, обрабатываемая в ПУТР .....  | 12 |
| Персональные данные.....  | 12 |
| Конфиденциальная информация .....   | 13 |
| Общедоступная информация .....  | 13 |
| 2.6. Объекты защиты.....  | 13 |
| 3. Модель нарушителя информационной безопасности.....                                 | 13 |
| 3.1. Общие положения .....  | 13 |
| 3.2. Описание нарушителей.....  | 13 |
| 3.3. Предположения об имеющихся у нарушителей средствах атак .....                    | 14 |
| 3.4. Предположения об имеющихся у нарушителей средствах атак .....                    | 16 |
| 3.5. Описание каналов атак .....  | 17 |

|   |    |
|---|----|
| 4. Модель угроз .....                       | 17 |
| 4.1. Общие положения .....                  | 17 |
| 5. Меры по противодействию угрозам ИБ ..... | 17 |
| 6. Заключение .....                         | 23 |

**ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ**

|             |   |   |
|-------------|---|---|
| <b>БД</b>   | – | База данных   |
| <b>ЖЦ</b>   | – | Жизненный цикл  |
| <b>ИБ</b>   | – | Информационная безопасность   |
| <b>ИС</b>   | – | Информационная система управления правами на результаты интеллектуальной деятельности |
| <b>ИТ</b>   | – | Информационные технологии   |
| <b>НСД</b>  | – | Несанкционированный доступ  |
| <b>ПДн</b>  | – | Персональные данные   |
| <b>ПО</b>   | – | Программное обеспечение   |
| <b>СВТ</b>  | – | Средства вычислительной техники   |
| <b>СЗИ</b>  | – | Система защиты информации   |
| <b>СОИБ</b> | – | Система обеспечения информационной безопасности                                       |
| <b>СрЗИ</b> | – | Средство защиты информации  |
| <b>ТС</b>   | – | Техническое средство  |
| <b>ПУТР</b> | – | Подсистема управления требованиями  |

## Термины и определения

|   |   |
|---|---|
| <b>Атака</b>                            | Целенаправленные действия нарушителя с использованием технических и (или) программных средств с целью нарушения заданных характеристик безопасности защищаемой информации или с целью создания условий для этого. |
| <b>Безопасность информации (данных)</b> | Состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность.   |
| <b>Защищаемая информация</b>            | Информация, для которой обладателем информации определены характеристики ее безопасности.   |
| <b>Информационная система</b>           | Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.  |
| <b>Информация</b>                       | Сведения (сообщения, данные) независимо от формы их представления   |
| <b>Канал атаки</b>                      | Среда переноса от субъекта к объекту атаки (а, возможно, и от объекта к субъекту атаки) действий, осуществляемых при проведении атаки.  |
| <b>Конфиденциальная информация</b>      | Информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.                          |
| <b>Конфиденциальность информации</b>    | Обязательное для выполнения требование не передавать такую информацию третьим лицам без согласия ее обладателя лицом, получившим доступ к определенной информации.  |
| <b>Модель нарушителя</b>                | Предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.  |
| <b>Модель угроз</b>                     | Физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.   |

|   |  |
|---|--|
| <b>Нарушитель<br/>(субъект атаки)</b>                             | Лицо (или иницируемый им процесс), проводящее (проводящий) атаку.  |
| <b>Регистрация<br/>данных</b>                                     | Ввод данных пользователем в формы, предоставляемые интерфейсом пользователя ИС.  |
| <b>Роль</b>   | Совокупность функциональных возможностей (привилегий) пользователя ИС, позволяющая разграничивать доступ к различным функциям ИС. Соответствие ролям пользователей определенных функциональных возможностей определяется моделью определения прав доступа. |
| <b>Средство защиты<br/>информации</b>                             | Техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.  |
| <b>Угроза<br/>информационной<br/>безопасности<br/>организации</b> | Совокупность факторов и условий, создающих опасность нарушения информационной безопасности организации, вызывающую или способную вызвать негативные последствия (ущерб/вред) для организации.  |



## **1. Общие положения**

### ***1.1. Цели создания модели угроз и модели нарушителя информационной безопасности***

Целью создания модели угроз ИБ и модели нарушителя ИБ ПУТР является формирование единого перечня угроз и мер по противодействию им в рамках ПУТР.

### ***1.2. Область применения***

Настоящая модель угроз ИБ и модель нарушителя ИБ предназначена для определения состава мер по защите информации в ПУТР.

Модель угроз ПУТР должна учитываться при построении СЗИ ПУТР.

### ***1.3. Общие принципы формирования***

Разработка модели угроз ИБ ПУТР основывается на следующих принципах:

- При формировании модели угроз необходимо учитывать угрозы, осуществляющие нарушение безопасности информации (далее по тексту – прямая угроза), а также угрозы, создающие условия для появления прямых угроз (далее – косвенные угрозы).
- Защищаемая информация обрабатывается и хранится в ПУТР с использованием определенных информационных технологий и технических средств, порождающих объекты защиты различного уровня, атаки на которые создают прямые или косвенные угрозы защищаемой информации.

### ***1.4. Правила пересмотра***

Настоящая модель угроз ИБ и модель нарушителя ИБ может уточняться, дополняться или изменяться в соответствии с установленным порядком. Основанием для пересмотра настоящего документа служат:

- Изменения законодательства РФ в области защиты информации.
- Изменения в информационной системе.

## 2. Описание ПУТР

### 2.1. Наименование информационной системы

**Наименование проекта:** Подсистема управления требованиями

**Условное обозначение:** ПУТР

### 2.2. Цели создания и назначение ПУТР

Подсистема управления требованиями предназначена для контроля действий разработки программного обеспечения.

ПУТР предназначена для:

- Управления контролем выполнения требований.
- Контроля качества выполняемых требований, сроков их выполнения.
- Изменения требований.
- Аналитики и принятия решений.

Цели создания ПУТР:

- Сокращение времени анализа требований для аналитика;
- Сокращение времени анализа требований для тестировщика;
- В рамках подсистемы требований разработать функциональность для установки статуса требований пользователем;
- В рамках подсистемы требований разработать функциональность для изменения требований пользователем;

### 2.3. Общее описание архитектуры ПУТР

ПУТР является многопользовательской ИС. По виду автоматизируемой деятельности ПУТР относится к системам управления, сбора, хранения, обработки и передачи информации.

Технические средства (ТС) ПУТР включает сервера БД, серверы приложений.

Информация, обрабатываемая в ПУТР, передается по защищенным каналам связи, в том числе при взаимодействии с пользователями, участвующими в процессе обработке защищаемой информации. ПУТР имеет подключение к сети Интернет.

ПУТР реализована в виде клиент-серверного приложения. Инфраструктура приложения может функционировать как на серверах Заказчика, так и на бесплатных хост серверах. Территориальное расположение серверов не представляет особой значимости, главным фактором является их доступность.

ПУТР разработан с использованием фреймворка Django на языке Python3.

Архитектура ПУТР опирается на следующие требования для функционирования сервера приложений:

- Операционная система сервера: 64-разрядная; Centos 7, Debian и более современные
- Процессор: Intel Core i5-4430 / AMD FX-6300, а также более современные
- Оперативная память: 8 GB ОЗУ
- Сеть: Широкополосное подключение к интернету
- Место на диске: 500 GB

А также требования к аппаратному обеспечению клиента:

- Операционная система на стороне клиента: Любая.
- Процессор: Intel Core i3, а также более современные
- Оперативная память: 4 GB ОЗУ
- Сеть: Широкополосное подключение к интернету
- Место на диске: 5 GB

#### ***2.4. Физические лица, имеющие доступ к компонентам ПУТР***

Возможности пользователя по взаимодействию с Системой и доступу к информации определяются интерфейсом, разработанным для каждой роли пользователей. В таблице 1 представлены категории ролей пользователей системы, имеющих доступ к ее ресурсам.

*Таблица 1 – Перечень ролей пользователей, имеющих доступ к ресурсам Системы*

| Категория                | Тип доступа  | Описание  |
|--------------------------|--|---|
| Системный администратор  | Доступ к серверным компонентам средствам ПУТР<br>Имеет полный доступ к функциональности и информационным ресурсам Системы. | Сотрудники организации, обеспечивающие функционирование сервера системы ПУТР.   |
| Администратор баз данных | Имеет полный доступ к данным, обрабатываемым системой.   | Сотрудники организации, осуществляющие выполнение работ по установке, настройке и администрированию используемых в АС СУБД. |
| Пользователь             | Имеют ограниченный доступ  |   |

| Категория                   | Тип доступа   | Описание |
|-----------------------------|---|----------|
|                             | к web-интерфейсу системы и предоставляемым им функциям.     |          |
| Пользователи смежных систем | Имеют доступ к полной информации по требованиям к проектам. |          |

## ***2.5.Информация, обрабатываемая в ПУТР***

В ПУТР обрабатывается информация следующих категорий:

- Иные категории персональных данных (ПДн), не отнесенные к специальным, биометрическим или общедоступным, в соответствии с пунктом 5 Постановления Правительства Российской Федерации № 1119 от 01.11.2012 г.

Постановление Правительства Российской Федерации от 13 февраля 2019 г. № 146 "Об утверждении правил организации и осуществления государственного контроля и надзора за обработкой персональных данных"

- информация, составляющая коммерческую тайну;
- сведения, составляющие служебную информацию ограниченного распространения (служебная тайна);

В ПУТР обработка речевой и видео информации не осуществляется.

### **Персональные данные**

Персональные данные включают в себя, в частности следующую информацию:

- Фамилию, имя, отчество (ФИО).
- Имя учетной записи пользователя.
- Адрес электронной почты.
- Должность.

### **Конфиденциальная информация**

К конфиденциальной информации, обрабатываемой в ПУТР, относятся сведения о проектах, релизах, спецификациях, требованиях.

## Общедоступная информация

В ПУТР не хранится общедоступная информация.

### 2.6. Объекты защиты

Защищаемыми ресурсами Системы являются:

- обрабатываемая и защищаемая в системе информация (файлы, записи БД);
- системное и прикладное ПО;
- технические средства обработки (клиентская рабочая станция пользователя, серверные машины и коммутационное оборудование);
- каналы связи, используемые для взаимодействия компонентов системы;

## 3. Модель нарушителя информационной безопасности

### 3.1. Общие положения

Модель нарушителя ИБ содержит описание предположений о возможностях нарушителя, которые он может использовать для разработки и проведения атак на компоненты ПУТР, а также об ограничениях на эти возможности.

### 3.2. Описание нарушителей

По отношению к месту проведения атак потенциальные нарушители подразделяются на два типа:

- Внешние – нарушители, осуществляющие атаки не имевшие и/или не имеющие авторизованного доступа к системе.
- Внутренние – нарушители из категорий I–IV, осуществляющие атаки имея определенный авторизованный доступ к системе.

Предполагается, что внешний нарушитель не может воздействовать на защищаемую информацию для целей нарушения безопасности ПДн, так как состав информации, хранимой и обрабатываемой в Системе, не представляет интереса для внешнего нарушителя.

Перечень категорий внутренних нарушителей информационной безопасности и имеющейся у них информации об объектах реализации угроз Системы приведен в таблице.

*Таблица 2 – Категории внутренних нарушителей безопасности информации*

| Категория   | Описание                | Имеющаяся у нарушителя информация об объектах реализации угроз |
|-------------|-------------------------|--|
| Категория I | Системный администратор | Информация о структуре данных,                                 |

|               |                              |   |
|---------------|------------------------------|---|
|               | Системы                      | используемых в процессе коммуникациями со связанными подсистемами. Параметры сетевой конфигурации настоящей системы и идентификационные данные системы. Информационное обеспечение системы. |
| Категория II  | Администратор баз данных     | Полный доступ к данным, обрабатываемым системой. Доступ к идентификационным данным пользователей системы.   |
| Категория III | Пользователь смежной системы | Полный доступ на чтение к данным проекта: Релизы, спецификации, требования  |
| Категория IV  | Пользователь                 | Информация о данных, обрабатываемых системой в соответствии с правами доступа, установленного для данного пользователя.   |

### ***3.3.Предположения об имеющихся у нарушителей средствах атак***

Внутренний нарушитель может использовать доступные в свободной продаже технические средства и ПО, специально разработанные технические средства и ПО.

Таблица 3 – Соответствие между ролями пользователей в системе и категориями нарушителей

| Предположения о наличии информации                                    | Категория нарушителя |                         |                  |                             |              |
|---|----------------------|-------------------------|------------------|-----------------------------|--------------|
|   | Внешний              | Внутренний              |                  |                             |              |
|   |                      | 1                       | 2                | 3                           | 4            |
|   |                      | Системный администратор | Администратор БД | Пользователи смежных систем | Пользователь |
| Части защищаемой информации, передаваемой по внутренним каналам       | –                    | +                       | +                | -                           | -            |
| Имена учетных записей зарегистрированных пользователей (без паролей)  | –                    | +                       | +                | -                           | -            |
| Не менее одной связки <имя, пароль УЗ> для доступа к подсистемам ИС   | –                    | +                       | +                | +                           | +            |
| Полная информация о системном и прикладном ПО, используемом в ИС      | –                    | +                       | +                | -                           | -            |
| Информация об алгоритмах и программах обработки защищаемой информации | +                    | +                       | +                | +                           | +            |
| Парольная информация для административного доступа к компонентам ИС   | –                    | +                       | -                | -                           | -            |
| Сведения о линиях связи, по которым передается защищаемая информация  | –                    | +                       | +                | -                           | -            |
| Журнал событий ИБ компонента ИС                                       | –                    | +                       | -                | -                           | -            |
| Журнал событий СЗИ  | –                    | +                       | +                | -                           | -            |
| Все проявляющиеся в ИС нарушения правил эксплуатации СЗИ              | –                    | +                       | +                | -                           | -            |

### 3.4.Предположения об имеющихся у нарушителей средствах атак

Потенциальные нарушители различных типов обладают различным уровнем доступа к компонентам ИС, а также различным уровнем квалификации. Таким образом, следует классифицировать нарушителей относительно имеющихся у них средств атак. Предположения об имеющихся у нарушителей средствах атак представлены в таблице **Error! Reference source not found..**

Таблица 4 – Предположения об имеющихся у нарушителей средствах атак

| Предположения о наличии информации   | Категория нарушителя |                         |                  |                             |              |
|--|----------------------|-------------------------|------------------|-----------------------------|--------------|
|  | Внешний              | Внутренний              |                  |                             |              |
|  |                      | 1                       | 2                | 3                           | 4            |
|  |                      | Системный администратор | Администратор БД | Пользователи смежных систем | Пользователь |
| Доступное в свободной продаже ПО   | +                    | +                       | +                | +                           | +            |
| Специально разработанные технические средства и программное обеспечение (в том числе снифферы и программ анализа защищенности (сетевых сканеров безопасности)) | +                    | +                       | +                | -                           | -            |



---

### 3.5. Описание каналов атак

Для осуществления доступа к ресурсам Системы внутренний нарушитель может использовать следующие каналы атак:

- физический доступ к штатным программно-аппаратным средствам системы;
- носители информации, в том числе съемные.

Возможны следующие способы атак:

- негласное (скрытое) временное изъятие или хищение съемных носителей защищаемой информации, аутентифицирующей или ключевой информации;
- вызывание сбоев технических средств;
- внесение неисправностей в технические средства.

## 4. Модель угроз

### 4.1. Общие положения

В данном разделе содержится структурированный перечень угроз ИБ с привязкой к потенциальным нарушителям ИБ, способным реализовать эти угрозы.



Структурированный\_  
перечень\_угроз\_ИБ\_Г

[Ссылка на таблицу с моделями угроз и нарушителями ИБ \(файл «Структурированный перечень угроз ИБ ПУТР.xls»\)](#)

## 5. Меры по противодействию угрозам ИБ

Перечень мероприятий для противодействия угрозам предполагает использование мер как технического, так и организационного порядка в отношении угроз, степень опасности которых не ниже высокой. Предлагаемые мероприятия направлены на обеспечение защиты ресурсов в целях снижения негативных последствий при реализации угроз.

Описание мероприятий по защите ресурсов представлено в таблице 5.

Таблица 5 - Описание мероприятий по защите ресурсов

| №<br>п/п | Наименование угрозы  | Меры по защите от угроз  |   |
|----------|--|--|---|
|          |  | Организационные  | Технические   |
| 1.       | Угроза анализа криптографических алгоритмов и их реализации  | Использование актуальных версий сертифицированных средств криптографической защиты информации.   | Своевременная установка обновлений программного обеспечения, направленного на устранение выявленных уязвимостей ПО      |
| 2.       | Угроза доступа к локальным файлам сервера при помощи URL   | Использование сертифицированного программного обеспечения и средств защиты информации. Мониторинг информации об обнаружении уязвимостей используемого ПО и выпуске соответствующих исправлений.  | Своевременная установка обновлений программного обеспечения, направленного на устранение выявленных уязвимостей ПО      |
| 3.       | Угроза использования информации идентификации/аутентификации, заданной по умолчанию  | Инвентаризация и анализ установленного на серверах программного обеспечения на предмет наличия учетных записей «по умолчанию»  | Блокирование встроенных учетных записей с администраторскими правами  |
| 4.       | Угроза неправомерного ознакомления с защищаемой информацией  | Определение перечня лиц, допущенных в помещение, где расположены компоненты ГИС. Использование плотных штор или жалюзи на окнах. Меры по получению доступа в помещение. Ручная блокировка экрана | Автоматическая блокировка экрана по достижении заданного времени не активности.   |
| 5.       | Угроза неправомерных действий в каналах связи  |  | Защита шифровальными (криптографическими) методами каналов передачи данных  |
| 6.       | Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети | Мониторинг состояния средств межсетевого экранирования и фильтрации сетевого трафика   | Исключение средствами межсетевого экранирования доступа из внешних сетей к активному сетевому оборудованию, установка в |

|     |   |   |  |
|-----|---|---|--|
|     |   |   | настройках оборудования разрешения на администрирование устройств только с определенного пула адресов, принадлежащих внутренней сети организации |
| 7.  | Угроза несанкционированного удаления защищаемой информации                          | Определение перечня лиц, допущенных в помещение, где расположены компоненты ГИС   | Минимизация прав пользователей в системе   |
| 8.  | Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб | Мониторинг состояния средств межсетевого экранирования и фильтрации сетевого трафика  |  |
| 9.  | Угроза обхода некорректно настроенных механизмов аутентификации                     | Использование сертифицированного программного обеспечения и средств защиты информации. Мониторинг информации об обнаружении уязвимостей используемого ПО и выпуске соответствующих исправлений. | Своевременная установка обновлений программного обеспечения, направленного на устранение выявленных уязвимостей ПО                               |
| 10. | Угроза перехвата данных, передаваемых по вычислительной сети                        |   | Защита шифровальными (криптографическими) методами каналов передачи данных   |
| 11. | Угроза подмены действия пользователя путём обмана                                   | Разработка инструкции по работе в системе, доведение ее до пользователей  | Минимизация прав пользователей в системе   |
| 12. | Угроза включения в проект не достоверно испытанных компонентов                      | Использование сертифицированного программного обеспечения и средств защиты информации. Мониторинг информации об обнаружении уязвимостей используемого ПО и выпуске соответствующих исправлений. |  |
| 13. | Угроза заражения компьютера при посещении неблагонадёжных сайтов                    |   | Регулярное обновление вирусных дефиниций АВПО на серверах и АРМ пользователей, использование на сервере АВПО                                     |

|     |   |  |   |
|-----|---|--|---|
|     |   |  | отличного по производителю от АВПО, установленного на АРМах пользователей.  |
| 14. | Угроза «кражи» учётной записи доступа к сетевым сервисам                | Мониторинг состояния средств межсетевого экранирования и фильтрации сетевого трафика                                       | Настройка соответствующих правил на межсетевом экране   |
| 15. | Угроза неправомерного шифрования информации                             |  | Регулярное обновление вирусных дефиниций АВПО на серверах и АРМ пользователей, использование на сервере АВПО отличного по производителю от АВПО, установленного на АРМах пользователей.<br>Регулярное полное резервное копирование данных. Глубина копирования – не более одного дня. |
| 16. | Угроза скрытного включения вычислительного устройства в состав бот-сети | Использование сертифицированного программного обеспечения  | Регулярное обновление вирусных дефиниций АВПО на серверах и АРМ пользователей, использование на сервере АВПО отличного по производителю от АВПО, установленного на АРМах пользователей  |
| 17. | Угроза «фишинга»:   | Информирование пользователей о методах и средствах «фишинга». Регламентация доступа пользователей к ресурсам сети Интернет |   |
| 18. | Угроза отказа подсистемы обеспечения температурного режима              | Разработка инструкции по действиям сотрудников охраны в случае срабатывания датчика по превышению температуры в            | Оснащение серверного помещения основным и резервным кондиционером,  |

|     |   |  |  |
|-----|---|--|--|
|     |   | серверном помещении  | установка сигнального датчика и вывод тревожного сигнала на пост охраны здания организации   |
| 19. | Угроза внедрения вредоносного кода через рекламу, сервисы и контент   |  | Регулярное обновление вирусных дефиниций АВПО на серверах и АРМ пользователей, использование на сервере АВПО отличного по производителю от АВПО, установленного на АРМах пользователей |
| 20. | Угроза подмены программного обеспечения   | Использование сертифицированного программного обеспечения  |  |
| 21. | Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет:                             |  | Регулярное обновление вирусных дефиниций АВПО на серверах и АРМ пользователей, использование на сервере АВПО отличного по производителю от АВПО, установленного на АРМах пользователей |
| 22. | Угроза использования уязвимых версий программного обеспечения   | Использование сертифицированного программного обеспечения и средств защиты информации. Мониторинг информации об обнаружении уязвимостей используемого ПО и выпуске соответствующих исправлений | Своевременная установка обновлений программного обеспечения, направленного на устранение выявленных уязвимостей ПО   |
| 23. | Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения | Мониторинг информации об обнаружении уязвимостей используемого ПО и выпуске соответствующих исправлений Использование официальных источников обновлений.                                       | Регулярное резервное копирование данных.   |
| 24. | Угроза перехвата управления информационной системой   | Использование сертифицированного   | Своевременная установка  |

|     |   |  |  |
|-----|---|--|--|
|     |   | программного обеспечения и средств защиты информации. Мониторинг информации об обнаружении уязвимостей используемого ПО и выпуске соответствующих исправлений. | обновлений программного обеспечения, направленного на устранение выявленных уязвимостей ПО. Регулярное обновление вирусных дефиниций АВПО на серверах. Защита шифровальными (криптографическими) методами каналов передачи данных.                                       |
| 25. | Угроза воздействия на программы с высокими привилегиями                     | Инвентаризация и анализ установленного на серверах программного обеспечения на предмет наличия учетных записей «по умолчанию»                                  | Блокирование встроенных учетных записей с администраторскими правами   |
| 26. | Угроза искажения вводимой и выводимой на периферийные устройства информации | Мониторинг состояния средств межсетевого экранирования и фильтрации сетевого трафика   | Исключение средствами межсетевого экранирования доступа из внешних сетей к активному сетевому оборудованию, установка в настройках оборудования разрешения на администрирование устройств только с определенного пула адресов, принадлежащих внутренней сети организации |

## 6. Заключение

Представленная в данном документе Модель угроз и нарушителей информационной безопасности ИС должна использоваться при реализации системы, в ходе ее внедрения и эксплуатации.

В соответствии порядком ввода и обработки информации, реализуемом в ИС, на протяжении опытной и промышленной эксплуатации в ИС будет обрабатываться и храниться информация, составляющая:

- Персональные данные, не отнесенные к специальным, биометрическим или общедоступным;
- Коммерческую тайну;
- Служебную информацию ограниченного распространения и ей организаций.

На протяжении опытной и постоянной эксплуатации в ИС не должна образовываться и содержаться информация:

- Подлежащая засекречиванию.
- Отнесенная к выполнению заказов на поставку товаров, выполнение работ или оказание услуг для государственных нужд (раскрывающая государственные заказы).

Для обеспечения конфиденциальности, целостности и доступности указанной информации необходимо принятие мер по обеспечению безопасности информации, предусмотренных законодательством РФ и нормативными документами.

В V главе приведены примеры с возможными способами их предотвращения или эскалации, для полной информации обо всех возможных угрозах для данной ИС следует посмотреть банк угроз.