|  |  |  |
| --- | --- | --- |
|  |  |  |
| Подсистема управления требованиями  Модель угроз информационной безопасности  Версия 1.0 | | |
| **СОГЛАСОВАНО** |  | **Представители организации Разработчика** |
| Должность  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Х.Х. ХХХХ  (личная подпись) (расшифровка подписи)  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_2021 г |  | Должность  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Х.Х. ХХХХ  (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](#_Toc61983213)

[1. Общие положения 9](#_Toc61983214)

[1.1. Цели создания модели угроз и модели нарушителя информационной безопасности 9](#_Toc61983215)

[1.2. Область применения 9](#_Toc61983216)

[1.3. Общие принципы формирования 9](#_Toc61983217)

[1.4. Правила пересмотра 9](#_Toc61983218)

[2. Описание ПУТР 10](#_Toc61983219)

[2.1. Наименование информационной системы 10](#_Toc61983220)

[2.2. Цели создания и назначение ПУТР 10](#_Toc61983221)

[2.3. Общее описание архитектуры ПУТР 10](#_Toc61983222)

[2.4. Физические лица, имеющие доступ к компонентам ПУТР 11](#_Toc61983223)

[2.5. Информация, обрабатываемая в ПУТР 12](#_Toc61983224)

[Персональные данные 12](#_Toc61983225)

[Конфиденциальная информация 13](#_Toc61983226)

[Общедоступная информация 13](#_Toc61983227)

[2.6. Объекты защиты 13](#_Toc61983228)

[3. Модель нарушителя информационной безопасности 13](#_Toc61983229)

[3.1. Общие положения 13](#_Toc61983230)

[3.2. Описание нарушителей 13](#_Toc61983231)

[3.3. Предположения об имеющихся у нарушителей средствах атак 14](#_Toc61983232)

[3.4. Предположения об имеющихся у нарушителей средствах атак 16](#_Toc61983233)

[3.5. Описание каналов атак 17](#_Toc61983234)

[4. Модель угроз 17](#_Toc61983235)

[4.1. Общие положения 17](#_Toc61983236)

[5. Меры по противодействию угрозам ИБ 17](#_Toc61983237)

[6. Заключение 23](#_Toc61983238)

Обозначения и сокращения

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

Термины и определения

|  |  |  |  |
| --- | --- | --- | --- |
| **Атака** | 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. | | |
| **Безопасность информации (данных)** | Состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность. | | |
| **Защищаемая информация** | Информация, для которой обладателем информации определены характеристики ее безопасности. | | |
| **Информационная система** | Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. | | |
| **Информация** | Сведения (сообщения, данные) независимо от формы их представления | | |
| **Канал атаки** | Среда переноса от субъекта к объекту атаки (а, возможно, и от объекта к субъекту атаки) действий, осуществляемых при проведении атаки. |
| **Конфиденциальная информация** | Информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации. | | |
| **Конфиденциальность информации** | Обязательное для выполнения требование не передавать такую информацию третьим лицам без согласия ее обладателя лицом, получившим доступ к определенной информации. | | |
| **Модель нарушителя** | Предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности. | | |
| **Модель угроз** | Физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации. | | |
| **Нарушитель (субъект атаки)** | Лицо (или инициируемый им процесс), проводящее (проводящий) атаку. | | |
| **Регистрация данных** | Ввод данных пользователем в формы, предоставляемые интерфейсом пользователя ИС. | | |
| **Роль** | Совокупность функциональных возможностей (привилегий) пользователя ИС, позволяющая разграничивать доступ к различным функциям ИС. Соответствие ролям пользователей определенных функциональных возможностей определяется моделью определения прав доступа. | | |
| **Средство защиты информации** | Техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации. | |
| **Угроза информационной безопасности организации** | Совокупность факторов и условий, создающих опасность нарушения информационной безопасности организации, вызывающую или способную вызвать негативные последствия (ущерб/вред) для организации. | | |
|  |  | | |
|  |  | | |

# Общие положения

## 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.

## 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.

## Общие принципы формирования

Разработка модели угроз ИБ ПУТР основывается на следующих принципах:

* При формировании модели угроз необходимо учитывать угрозы, осуществляющие нарушение безопасность 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.

## 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.

# Описание ПУТР

## Наименование информационной системы

**Наименование проекта:** Подсистема управления требованиями

**Условное обозначение**: ПУТР

## 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;

## 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

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

## 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.

## 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;

# Модель нарушителя информационной безопасности

## 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.

## 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 Системы | Информация о структуре данных, 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. |

## 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.

| **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 | **–** | **+** | **-** | **-** | **-** |

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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 | **–** | **+** | **+** | **-** | **-** |

## 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 4.

*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)) | **+** | **+** | **+** | **-** | **-** |

## 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.

# Модель угроз

## Общие положения

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



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

# 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*

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование угрозы | Меры по защите от угроз | |
| Организационные | Технические |
|  | 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 |
|  | 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 |
|  | 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 |
|  | 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. |
|  | Угроза неправомерных действий в каналах связи |  | Защита шифровальными (криптографическими) методами каналов передачи данных |
|  | 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 |
|  | Угроза несанкционированного удаления защищаемой информации | Определение перечня лиц, допу­щенных в помещение, где расположены компоненты ГИС | Минимизация прав пользователей в системе |
|  | Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб | Мониторинг состояния средств межсетевого экранирования и фильтрации сетевого трафика |  |
|  | 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 |
|  | Угроза перехвата данных, передаваемых по вычислительной сети |  | Защита шифровальными (криптографическими) методами каналов передачи данных |
|  | Угроза подмены действия пользователя путём обмана | Разработка инструкции по работе в системе, доведение ее до пользователей | Минимизация прав пользователей в системе |
|  | 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. |  |
|  | 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. |
|  | Угроза «кражи» учётной записи доступа к сетевым сервисам | Мониторинг состояния средств межсетевого экранирования и фильтрации сетевого трафика | Настройка соответствующих правил на межсетевом экране |
|  | 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.  Регулярное полное резервное копирование данных. Глубина копирования – не более одного дня. |
|  | 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 |
|  | Угроза «фишинга»: | Информирование пользователей о методах и средствах «фишинга». Регламентация доступа пользователей к ресурсам сети Интернет |  |
|  | Угроза отказа подсистемы обеспечения температурного режима | Разработка инструкции по действиям сотрудников охраны в случае срабатывания датчика по превышению температуры в серверном помещении | Оснащение серверного помещения основным и резервным кондиционером, установка сигнального датчика и вывод тревожного сигнала на пост охраны здания организации |
|  | 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 |
|  | Угроза подмены программного обеспечения | Использование сертифицированного программного обеспечения |  |
|  | 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 |
|  | 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 |
|  | 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 обновлении. | Регулярное резервное копирование данных. |
|  | Угроза перехвата управления информационной системой | 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. Регулярное обновление вирусных дефиниций АВПО на серверах. Защита шифровальными (криптографическими) методами каналов передачи данных. |
|  | 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 |
|  | 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 |

# Заключение

Представленная в данном документе 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.