ИНФОРМАЦИОННАЯ СИСТЕМА

**МОДЕЛЬ УГРОЗ И НАРУШИТЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИС**

|  |  |
| --- | --- |
| **СОГЛАСОВАНО**  Генеральный директор  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2020 г. | **СОГЛАСОВАНО**  Генеральный директор  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2020 г. |
|  |  |

Москва

2020 г.

Лист согласований

Лист разработчиков

| Наименование организации | Должность | Инициалы и  фамилия | Подпись | Дата |
| --- | --- | --- | --- | --- |
|  |  |  |  | «\_\_\_»\_\_\_\_\_\_ 2020 г. |
|  |  |  |  | «\_\_\_»\_\_\_\_\_\_ 2020 г. |
|  |  |  |  | «\_\_\_»\_\_\_\_\_\_ 2020 г. |
|  |  |  |  | «\_\_\_»\_\_\_\_\_\_ 2020 г. |
|  |  |  |  | «\_\_\_»\_\_\_\_\_\_ 2020 г. |
|  |  |  |  | «\_\_\_»\_\_\_\_\_\_ 2020 г. |

Аннотация

В данном документе описывается модель угроз и модель нарушителя информационной безопасности информационной системы управления правами на результаты интеллектуальной деятельности (ИС).

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

Модель угроз информационной безопасности ИС содержит:

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

Содержание

[Обозначения и сокращения 6](#_Toc468310796)

[Термины и определения 7](#_Toc468310797)

[1 Общие положения 9](#_Toc468310798)

[1.1 Цели создания модели угроз и модели нарушителя информационной безопасности 9](#_Toc468310799)

[1.2 Область применения 9](#_Toc468310800)

[1.3 Общие принципы формирования 9](#_Toc468310801)

[1.4 Правила пересмотра 9](#_Toc468310802)

[2 Описание ИС 9](#_Toc468310803)

[2.1 Наименование информационной системы 9](#_Toc468310804)

[2.2 Цели создания и назначение ИС 9](#_Toc468310805)

[2.3 Общее описание архитектуры ИС 10](#_Toc468310806)

[2.4 Физические лица, имеющие доступ к компонентам ИС 10](#_Toc468310807)

[2.5 Информация, обрабатываемая в ИС 10](#_Toc468310808)

[2.5.1 Персональные данные 10](#_Toc468310809)

[2.5.2 Конфиденциальная информация 11](#_Toc468310810)

[2.5.3 Общедоступная информация 11](#_Toc468310811)

[2.6 Объекты защиты 11](#_Toc468310812)

[3 Модель нарушителя информационной безопасности 12](#_Toc468310813)

[3.1 Общие положения 12](#_Toc468310814)

[3.2 Описание нарушителей 12](#_Toc468310815)

[3.3 Предположения об имеющейся у нарушителей информации об объектах атак 15](#_Toc468310816)

[3.4 Предположения об имеющихся у нарушителей средствах атак 18](#_Toc468310817)

[3.5 Описание каналов атак 19](#_Toc468310818)

[4 Модель угроз 21](#_Toc468310819)

[4.1 Общие положения 21](#_Toc468310820)

[4.2 Классификация угроз 21](#_Toc468310821)

[4.2.1 Виды угроз 21](#_Toc468310822)

[4.2.2 Источники угроз 22](#_Toc468310823)

[4.3 Объекты защиты 22](#_Toc468310824)

[4.4 Модель угроз 22](#_Toc468310825)

[4.4.1 Перечень угроз, не являющихся атаками 22](#_Toc468310826)

[4.4.2 Перечень угроз, являющихся атаками 24](#_Toc468310827)

[5 Меры по противодействию угрозам ИБ 27](#_Toc468310828)

[6 Заключение 40](#_Toc468310829)

Обозначения и сокращения

|  |  |  |
| --- | --- | --- |
| **БД** | − | База данных |
| **ДЗО** | − | Дочерние и зависимые общества |
| **ЗИП** | − | Запчасти и принадлежности |
| **ИБ** | − | Информационная безопасность |
| **ИС** | − | Информационная система управления правами на результаты интеллектуальной деятельности |
| **ИТ** | − | Информационные технологии |
| **КЗ** | − | Контролируемая зона |
| **НСД** | − | Несанкционированный доступ |
| **НСИ** | − | Нормативно-справочная информация |
| **ОТСС** | − | Основные технические средства и системы |
| **ПДн** | − | Персональные данные |
| **ПО** | − | Программное обеспечение |
| **СВТ** | − | Средства вычислительной техники |
| **СЗИ** | − | Система защиты информации |
| **СОИБ** | − | Система обеспечения информационной безопасности |
| **ТС** | − | Техническое средство |

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. | | |
| **Заказчик** |  |
| **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. | | |
| **Информационные технологии** | Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов. | | |
| **Информация** | Сведения (сообщения, данные) независимо от формы их представления | | |
| **Информация ограниченного доступа** | Информация, доступ к которой ограничен на основании законодательства Российской Федерации. | | |
| **Инцидент** | Любое событие, не являющееся частью нормальной работы услуги, ведущее/ способное привести к остановке услуги или снижению уровня её качества. | | |
| **Исполнитель** | 1. организация отрасли, или 2. организация вне отрасли, |
| **Канал атаки** | Среда переноса от субъекта к объекту атаки (а, возможно, и от объекта к субъекту атаки) действий, осуществляемых при проведении атаки. | | |
| **Контролируемая зона** | Пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств. Границей контролируемой зоны может быть: периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения. | | |
| **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. | | |
| **Опубликованные возможности ПО или ТС** | Возможности, сведения о которых содержатся в общедоступных открытых источниках (технические и любые другие материалы разработчика ПО или ТС, монографии, публикации в средствах массовой информации (СМИ), материалы конференций и других форумов, информация из сети Internet и т.д.). | | |
| **Основные технические средства и системы обработки конфиденциальной информации** | Средства вычислительной техники, на которых обрабатывается конфиденциальная информация | | |
| **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 вычислительной техники** | Совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем. | | |
| **Средство защиты информации** | Техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации. | | |
| **Угроза безопасности объекта** | Возможное нарушение характеристики безопасности объекта. | | |
| **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 информационной безопасности (ИБ) и модели нарушителя ИБ ИС является формирование единого перечня угроз и мер по противодействию им в рамках ИС.

## Область применения

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

Модель угроз ИС должна учитываться при построении СЗИ ИС.

## Общие принципы формирования

Разработка модели угроз ИБ ИС базируется на следующих принципах:

* При формировании модели угроз необходимо учитывать как угрозы, осуществление которых нарушает безопасность информации (далее – прямая угроза), так и угрозы, создающие условия для появления прямых угроз (далее – косвенные угрозы).
* Защищаемая информация обрабатывается и хранится в ИС 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 ИС

## Наименование информационной системы

Полное наименование: Информационная система управления правами на результаты интеллектуальной деятельности.

Краткое наименование: ИС.

## Цели создания и назначение ИС

Сокращение времени организации процесса управления проектами и задачами со стороны пользователя, сокращение времени организации процесса управления проектами и задачами со стороны руководителя, мониторинг производительности пользователей.

## Общее описание архитектуры ИС

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

Технические средства (ТС) ИС включает серверы баз данных и приложений. Информация, обрабатываемая в ИС, передается по защищенным каналам связи, в том числе при взаимодействии с пользователями, участвующими в процессе обработке защищаемой информации. ИС имеет подключение к сетям связи общего пользования, в том числе к Интернет.

ИС реализована на физической инфраструктуре. Инфраструктура размещена в помещении с контролем доступа.

## Физические лица, имеющие доступ к компонентам ИС

Доступ к компонентам ИС осуществляется лицами следующих категорий:

* Администраторы ИТ – работники, имеющие санкционированный ограниченный доступ к ИТ–компонентам ИС (с локальной консоли или удаленно с рабочего места).
* Администраторы ИБ – работники, имеющие санкционированный ограниченный доступ к ИБ–компонентам ИС (с локальной консоли или удаленно с рабочего места).
* Функциональные пользователи – работники, имеющие санкционированный ограниченный доступ к функциональным компонентам ИС, в том числе к защищаемой информации;
* Эксплуатационный персонал – работники, имеющие санкционированный доступ к техническим компонентам, на базе которых функционирует ИС, но не имеющие доступа к защищаемой информации.

## Информация, обрабатываемая в ИС

В ИС 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.
* информация, составляющая коммерческую тайну;
* сведения, составляющие служебную информацию ограниченного распространения (служебная тайна);
* общедоступная информация.

В ИС обработка речевой и видео информации не осуществляется.

### Персональные данные

Персональные данные, обрабатываемые в ИС, представляют собой. Персональные данные включают в себя, в частности следующую информацию:

* Фамилию, имя, отчество (ФИО).
* Имя учетной записи пользователя.
* Адрес электронной почты.
* Прочая контактная информация.
* Предприятие.
* Подразделение.
* Должность.

### Конфиденциальная информация

К конфиденциальной информации, обрабатываемой в ИС, относится:

* Сведения, раскрывающие конкретные параметры планируемых мероприятий, направленных на привлечение и концентрацию интеллектуальных, производственных и финансовых ресурсов с целью реализации перспективных программ повышения конкурентоспособности продукции и дочерних и зависимых обществ (ДЗО).
* Сведения, раскрывающие вопросы ценообразования по проектам, находящимся в стадии согласования с конкретным российским или иностранным партнером.
* Перечень результатов интеллектуальной деятельности по проектам, реализуемым в рамках соответствующих межправительственных соглашений, в которых предусматривается использование предшествующей интеллектуальной собственности предприятий и организаций Корпорации.
* Сведения об оригинальных, незапатентованных технических (конструктивных и технологических) решениях, предполагаемых к применению или применяемых в производстве продукции, и обеспечивающих заметное повышение технико-экономических показателей.
* Результаты расчетно-теоретических и фактические показатели экспериментальных работ по технологиям и продуктам, имеющим приоритетное коммерческое значение для Корпорации.
* Информация, раскрывающая планы предприятий Корпорации по выпуску конкурентоспособных товаров и услуг, за исключением государственных контрактов и ИТ-продукции.
* Сведения, раскрывающие результаты экспертиз (экспертных заключений), проведенных в интересах Корпорации, в области инновационных решений, позволяющих повысить конкурентоспособность продукции, если в заключениях содержится описание инновации.

Конфиденциальная информация, хранимая и обрабатываемая в ИС, доступна пользователям системы через пользовательский интерфейс, в частности через такие объекты системы как: «Карточка», а также через связанные с этими объектами документами, размещенными в системе. Пользователи с правами администратора НСИ имеет также доступ к нормативно-справочной информации, потенциально также носящей конфиденциальный характер. Администраторы БД могут реализовать доступ к хранимой в БД ИС конфиденциальной информации через непосредственное подключение к БД, минуя интерфейс системы. Администраторы ИБ имеют доступ к информации о правах доступа пользователей к системе через интерфейс модуля администрирования, а также имеет возможность изменить пароль пользователя.

### Общедоступная информация

В ИС не хрангится общедоступной информации.

## Объекты защиты

Объектами защиты в ИС являются:

* Информационные ресурсы в виде информационных массивов и баз данных, содержащих защищаемую информацию, и представленные на магнитных, оптических и других носителях, а также передаваемые по каналам связи.
* Основные технические средства и системы (ОТСС) обработки конфиденциальной информации – средства вычислительной техники (СВТ), на которых обрабатывается конфиденциальная информация, включая серверы, коммуникационное оборудование и линии связи.
* Программные и аппаратные компоненты системы защиты информации.
* Съемные носители конфиденциальной информации.
* Серверные помещения.
* Ключевая, аутентифицирующая и парольная информация.
* Конфигурационная информация.
* Остаточная информация на носителях информации.

# Модель нарушителя информационной безопасности

## Общие положения

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

## Описание нарушителей

Все физические лица, имеющие доступ к техническим и программным средствам ИС, разделяются на следующие категории:

* категория I – лица, не имеющие права доступа в контролируемую зону установки ИС;
* категория II – лица, имеющие право постоянного или разового доступа в контролируемую зону установки ИС.

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

* Внешние – нарушители, осуществляющие атаки из-за пределов контролируемой зоны.
* Внутренние – нарушители, осуществляющие атаки, находясь в пределах контролируемой зоны.

Таким образом, можно констатировать, что:

* Внешними нарушителями могут быть как лица категории I, так и лица категории II.
* Внутренними нарушителями могут быть только лица категории II.

В качестве потенциальных внешних нарушителей информационной безопасности ИС теоретически могут рассматриваться:

* Криминальные структуры.
* Недобросовестные партнеры.
* Внешние субъекты (физические лица), в том числе хакеры.
* Работники, находящиеся за пределами контролируемой зоны.

Следующих потенциальных внешних нарушителей рекомендуется исключить из рассмотрения (см. таблицу 2).

*Таблица 1 – Обоснование исключения из рассмотрения части внешних нарушителей*

| **Тип внешнего нарушителя** | **Обоснование исключения из рассмотрения** |
| --- | --- |
| Криминальные структуры | Предполагается, что криминальные структуры для реализации угроз ИБ пользуются услугами хакеров. В связи с этим, возможности нарушителей данной категории ничем не отличаются от возможностей нарушителей типа «внешние субъекты (физические лица), в том числе хакеры». |
| Недобросовестные партнеры | Предполагается, что недобросовестные партнеры для реализации угроз ИБ пользуются услугами хакеров. В связи с этим, возможности нарушителей данной категории ничем не отличаются от возможностей нарушителей типа «внешние субъекты (физические лица), в том числе хакеры». |

Таким образом, в качестве внешнего нарушителя информационной безопасности ИС рекомендуется рассматривать внешних субъектов (физических лиц), в том числе хакеров, а также работников, находящихся за пределами контролируемой зоны.

В качестве внутренних потенциальных нарушителей, в зависимости от способа и полномочий доступа к ИС, могут рассматриваться нарушители следующих типов:

* Тип 1 – лица, имеющие санкционированный доступ к компонентам ИС, но не имеющие доступа к защищаемой информации. К нарушителям этой категории относится обслуживающий персонал, обеспечивающий функционирование объекта информатизации.
* Тип 2 – зарегистрированные пользователи ИС, осуществляющие ограниченный доступ к ресурсам ИС с рабочего места. К нарушителям этой категории относятся работники, имеющие права доступа к подсистемам ИС для выполнения своих служебных обязанностей.
* Тип 3 – зарегистрированные пользователи ИС с полномочиями администратора ИТ (включая администрирование БД).
* Тип 4 – зарегистрированные пользователи с полномочиями администратора ИБ.
* Тип 5 – программисты–разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте (далее – поставщики ПО). На период проведения работ по вводу в эксплуатацию ИС временно обладают полномочиями всех ролей ИС.
* Тип 6 – разработчики и лица, обеспечивающие поставку, сопровождение и ремонт ТС ИС (далее – поставщики ТС).

Соответствие между ролями пользователей в системе и категориями (типами) нарушителей представлено в таблице 3.

Тип нарушителя 1 соответствует обслуживающему персоналу. Работы, связанные с уборкой, ремонтом и т.п., серверной площадки, где располагаются компоненты ИС, а так же контроль за посетителями, выполняются под надзором ответственных за пропускной режим лиц.

Тип нарушителя 2 соответствует работникам, принимаемым на работу на основе кадровых и организационно-штатных мероприятий, исключающих возможность несанкционированных действий со стороны данных лиц.

Типы нарушителей 3, 4, 5 и 6 соответствуют работникам, которые принимаются на работу или допускаются к работе на основе кадровых, организационно-штатных и прочих регламентированных мероприятий. Данные работники проходят инструктаж по вопросам обработки информации и специфике использования ИС. Допуск указанных лиц к работе с ресурсами и/или с ТС ИС предоставляется в случае заключения с ними соответствующих гарантийных соглашений, устанавливающих наступление персональной ответственности в случае совершения ими несанкционированных/ошибочных действий. Предполагается невозможность совершения указанными лицами несанкционированных, а также ошибочных действий.

Права доступа ролей к функциям ИС определены в документе B-NI1-1. Матрица доступа.

*Таблица 2 – Соответствие между ролями пользователей в системе и категориями нарушителей*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Роль в ИС** | **Категория нарушителя** | | | | | | |
| **Внешний** | **Внутренний** | | | | | |
| **1** | **2** | **3** | **4** | **5** | **6** |
| **Обслуж. персонал, посетители** | **Пользователи** | **Администраторы ИТ** | **Администраторы ИБ** | **Поставщики ПО** | **Поставщики ТС** |
| **Пользователь** | ‑ | ‑ | + | ‑ | ‑ | - | ‑ |
| **Руководитель** | ‑ | ‑ | + | ‑ | ‑ | - | ‑ |
| **Администратор** | ‑ | ‑ | + | + | + | - | ‑ |

## Предположения об имеющейся у нарушителей информации об объектах атак

Теоретически, указанные в подразделе 3.2 потенциальные нарушители могут обладать всей информацией, необходимой им для подготовки и проведения атак за исключением аутентифицирующей и ключевой информации. Принимая во внимание тот факт, что потенциальные нарушители различных типов обладают различным уровнем доступа к компонентам ИС, а также различным уровнем квалификации, следует дифференцировать нарушителей относительно доступной им информации об объектах атак. Предположения о наличии у нарушителей разного рода информации об объектах атак приведены в таблице 3.

*Таблица* *3* *– Предположения об имеющейся у нарушителей информации об объектах атак*

| **Предположения о наличии информации** | **Категория нарушителя** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Внешний** | **Внутренний** | | | | | |
| **1** | **2** | **3** | **4** | **5** | **6** |
| **Обслуж. персонал** | **Пользователи** | **Администраторы ИТ** | **Администраторы ИБ** | **Поставщики ПО** | **Поставщики ТС** |
| Фрагменты защищаемой информации, передаваемой по внутренним каналам | **–** | **+** | **+** | **+** | **+** | **+** | **+** |
| Фрагменты информации о топологии ИС, об используемых коммуникационных протоколах и сервисах, об используемых ПО, ТС, СЗИ | **+** | **+** | **+** | **+** | **+** | **+** | **+** |
| Имена учетных записей зарегистрированных пользователей (без паролей) | **–** | **+** | **+** | **+** | **+** | **+** | **+** |
| Как минимум, одно имя и пароль учетной записи для доступа к подсистемам ИС | **–** | **–** | **+** | **+** | **+** | **+** | **–** |
| Конфиденциальная информация, к которой имеется легальный доступ | **–** | **–** | **+** | **+** | **+** | **–** | **–** |
| Полная информация о системном и прикладном программном обеспечении, используемом в ИС | **–** | **–** | **–** | **+** | **+** | **+** | **–** |
| Полная информация о технических средствах и конфигурации ИС | **–** | **–** | **–** | **+** | **+** | **–** | **–** |
| Информация об алгоритмах и программах обработки защищаемой информации | **+** | **–** | **‑** | **+** | **+** | **+** | **–** |
| Содержание технической документации на технические и программные компоненты СЗИ ИС | **–** | **–** | **–** | **–** | **+** | **–** | **–** |
| Парольная информация для административного доступа к компонентам ИС | **–** | **–** | **–** | **+** | **+** | **–** | **–** |
| Сведения о линиях связи, по которым передается защищаемая информация | **–** | **–** | **–** | **+** | **+** | **–** | **–** |
| Журнал событий ИБ компонент ИС | **–** | **–** | **–** | **‑** | **+** | **–** | **–** |
| Журнал событий СЗИ | **–** | **–** | **–** | **–** | **+** | **–** | **–** |
| Все проявляющиеся в ИС нарушения правил эксплуатации СЗИ | **–** | **–** | **–** | **–** | **+** | **–** | **–** |
| Все проявляющиеся в ИС неисправности и сбои технических средств 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 дифференцировать 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 средств атак** | **Категория нарушителя** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Внешний** | **Внутренний** | | | | | |
| **1** | **2** | **3** | **4** | **5** | **6** |
| **Обслуж. персонал** | **Пользователи** | **Администраторы ИТ** | **Администраторы ИБ** | **Поставщики ПО** | **Поставщики ТС** |
| Доступные в свободной продаже технические средства и программное обеспечение | **+** | **+** | **+** | **+** | **+** | **+** | **+** |
| Специально разработанные технические средства и программное обеспечение (в том числе программ-анализаторов пакетов (снифферов) и программ анализа защищенности (сетевых сканеров безопасности)) | **+** | **–** | **–** | **+** | **+** | **+** | **+** |
| Штатные средства ПО компонентов ИС | **–** | **–** | **+** | **+** | **+** | **+** | **–** |
| Аппаратные компоненты СЗИ | **–** | **–** | **–** | **+** | **+** | **–** | **+** |

## Описание каналов атак

Набор каналов атак, доступных потенциальному нарушителю, определяется уровнем доступа нарушителя к компонентам ИС. В связи с этим следует дифференцировать нарушителей относительно доступных им каналов атак. Предположения о доступных нарушителям каналах атак приведены таблице 5.

*Таблица* *5 – Предположения о доступных нарушителям каналах атак*

| **Предположения о доступных каналах атак** | **Категория нарушителя** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Внешний** | **Внутренний** | | | | | |
| **1** | **2** | **3** | **4** | **5** | **6** |
| **Обслуж. персонал** | **Пользователи** | **Администраторы ИТ** | **Администраторы ИБ** | **Поставщики ПО** | **Поставщики ТС** |
| Штатные средства компонентов ИС | – | – | + | + | + | + | + |
| Штатные средства СЗИ | – | – | ‑ | ‑ | + | – | – |
| Каналы связи внутри КЗ | – | + | + | + | + | + | + |
| Физический доступ к серверам | – | + | – | + | + | + | + |
| Физический доступ к коммуникационному оборудованию | – | + | – | + | + | – | + |
| Физический доступ к СЗИ | – | – | – | + | + | + | + |
| Визуальный доступ | – | + | + | + | + | + | + |
| Машинные носители информации | – | + | + | + | + | + | + |
| Носители информации, вышедшие из употребления | + | + | + | + | + | + | + |
| Информационные и управляющие интерфейсы СВТ | – | – | + | + | + | + | + |

# Модель угроз

## Общие положения

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

## Классификация угроз

### Виды угроз

Относительно этапов жизненного цикла ИС или ее компонентов, на которых возможна реализация угроз информационной безопасности, угрозы подразделяются на следующие:

* Угрозы, реализуемые на этапах разработки, производства и транспортировки технических и программных средств ИС.
* Угрозы, реализуемые на этапе эксплуатации технических и программных средств ИС.

Относительно нарушения безопасности защищаемой информации угрозы подразделяются:

* Прямые – угрозы, осуществление которых нарушает безопасность информации.
* Косвенные – угрозы, осуществление которых создает условия для появления прямых угроз.

Относительно наличия злого умысла все угрозы информационной безопасности можно разделить на две категории:

* Угрозы, не являющиеся атакой.
* Атаки.

Целями атак являются:

* Нарушение конфиденциальности защищаемых ресурсов ИС.
* Нарушение целостности защищаемых ресурсов ИС.
* Нарушение доступности защищаемых ресурсов ИС.
* Нарушение недоказуемости (авторства) защищаемых ресурсов ИС.
* Создание условий для проведения атак.

Угрозы, не являющиеся атаками, в свою очередь, можно разделить на следующие категории:

* Угрозы, не связанные с деятельностью человека: стихийные бедствия и природные явления (землетрясения, наводнения, ураганы и т.п.).
* Угрозы социально-политического характера: забастовки, саботаж, локальные конфликты и т.п.
* Угрозы техногенного характера.
* Ошибочные действия и (или) нарушения тех или иных требований лицами, санкционировано взаимодействующими с возможными объектами угроз.

Настоящая модель угроз предназначена для разработки требований, определяющих организационно-режимные и программно-технические мероприятия по защите информации в ИС; в связи с чем угрозы, не связанные с деятельностью человека, а также угрозы социально-политического характера в рамках данной модели не рассматриваются.

### Источники угроз

Источники угроз информационной безопасности делятся на субъективные (зависят от действий физических лиц) и объективные (зависят от особенностей построения и технических характеристик оборудования и ПО, применяемых на защищаемом объекте).

К субъективным источникам угроз относятся:

* Внешний нарушитель.
* Внутренний нарушитель.
* Физические лица, имеющие санкционированный доступ к ИС, и не являющиеся нарушителями.

Описание потенциальных нарушителей информационной безопасности приведено в разделе 3.

К объективным источникам угроз относятся:

* Сбои в функционировании программных средств.
* Сбои в функционировании аппаратных средств.

## Объекты защиты

Объекты защиты перечислены в п. 2.10 настоящего документа.

## Модель угроз

### Перечень угроз, не являющихся атаками

Перечень угроз информационной безопасности, не являющихся атаками, приведен в таблице 6.

*Таблица* *6 – Перечень угроз, не являющихся атаками*

| **Идентификатор угрозы** | **Описание** |
| --- | --- |
| 1.1 | Непредумышленное искажение или удаление работником программно-аппаратных компонентов ИС. |
| 1.2 | Внедрение и использование работником неучтенного программного обеспечения, в том числе вредоносного. |
| 1.3 | Игнорирование работником организационных ограничений (установленных правил) при работе с информационными ресурсами ИС, включая СЗИ. |
| 1.3.1 | Нарушение правил хранения и передачи защищаемой информации. |
| 1.3.2 | Предоставление работником возможности доступа к компонентам ИС, а также самой информации посторонним лицам. |
| 1.3.3 | Настройка и конфигурирование пользователем компонент ИС в нарушение нормативных технических документов. |
| 1.3.4 | Утрата, компрометация пользователем ИС ключевой, парольной и аутентифицирующей информации, любой другой защищаемой информации, а также несообщение о фактах компрометации и утраты такой информации. |
| 1.4 | Сбои в функционировании программного обеспечения ИС. |
| 1.5 | Сбои в функционировании аппаратного обеспечения ИС. |
| 1.6 | Ошибки в проектировании ИС. |

### Перечень угроз, являющихся атаками

Перечень угроз информационной безопасности, являющихся атаками, приведен в таблице 7. Для каждой пары «угроза-нарушитель» на основании возможностей потенциального нарушителя данной категории: информация об объектах атак, имеющиеся средства атак, доступные каналы атак, ‑ делается вывод о возможности реализации им рассматриваемой угрозы.

*Таблица* *7 – Перечень угроз ИС, являющихся атаками*

| **Идентификатор угрозы** | **Описание угрозы** | | **Категория нарушителя** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Внешний** | **Внутренний** | | | | | |
| **1** | **2** | **3** | **4** | **5** | **6** |
| **Обслуж. персонал,** | **Пользователи** | **Администраторы ИТ** | **Администраторы ИБ** | **Поставщики ПО** | **Поставщики ТС** |
| **1** | **Угрозы несанкционированного доступа к информации** | | | | | | | | |
| 1.1. | Изменение параметров загрузки операционной системы (в том числе загрузка с внешних накопителей) | | – | – | – | + | + | + | + |
| 1.2. | Получение непосредственного доступа к компонентам СВТ | | – | ‑ | – | + | + | + | + |
| 1.3. | Кража носителей информации и мобильных устройств | | + | + | + | + | + | + | + |
| 1.4. | Восстановление информации с носителей, вышедших из употребления | | + | + | + | + | + | + | + |
| 1.5. | Порча или отключение критичных компонентов ИС | | – | + | – | + | + | + | + |
| 1.6. | Несанкционированное копирование конфиденциальной информации на внешние носители | | – | – | + | + | + | – | – |
| **2** | **Угрозы, реализуемые с использованием протоколов межсетевого взаимодействия** | | | | | | | | |
| 2.1. | Сканирование сети | | + | – | + | + | + | + | – |
| 2.2. | Подбор злоумышленником аутентифицирующей информации администраторов ИС | | + | + | + | + | + | + | + |
| 2.3. | Проведение атак типа «отказ в обслуживании» на каналы связи | | + | – | + | + | + | + | – |
| 2.4. | Проведение компьютерных атак на СВТ с целью получения несанкционированного доступа к программной среде СВТ | | + | – | + | + | + | + | – |
| 2.5. | Размещение защищаемой информации на незащищенных или не предназначенных для этих целей ресурсах ИС | | – | – | + | + | + | – | – |
| 2.6. | Передача защищаемой информации по сети за пределы КЗ | | – | – | + | + | + | – | – |
| 2.7. | Модификация защищаемой информации при ее передаче по каналам связи | | + | ‑ | + | + | + | ‑ | ‑ |
| **3** | **Угрозы программно–математических воздействий** | | | | | | | | |
| 3.1. | Внедрение вредоносного ПО (вирусов, троянов, backdoor и т.п.) | + | | – | + | + | + | + | – |
| **4** | **Угроз преднамеренных действий нарушителей** | | | | | | | | |
| 4.1. | Выявление сведений о структуре ИС, применяемых СВТ, средствах и подсистеме защиты обрабатываемой информации (использование методов «социальной инженерии») | + | | + | + | + | + | + | + |
| 4.2. | Публикация информации от имени другого пользователя ИС | ‑ | | ‑ | + | + | + | + | ‑ |
| 4.3. | Отказ от авторства передаваемой/ принимаемой информации | ‑ | | ‑ | + | + | + | + | ‑ |

# Меры по противодействию угрозам ИБ

Организационные и технические меры по противодействию угрозам информационной безопасности, на основании которых должны определяться требования к системе обеспечения информационной безопасности (СОИБ) ИС, в структурированном виде представлены в таблицах 8, 9.

*Таблица* *8 – Модель защиты информации ИС от угроз, не являющихся атаками*

| **№** | **Описание** | **Меры по противодействию** | |
| --- | --- | --- | --- |
| **Технические** | **Организационные** |
| **Угрозы, не являющиеся атаками** | | | |
| 1.1 | Непредумышленное искажение или удаление работником программно–аппаратных компонентов ИС | Использование средств резервного копирования и восстановления данных.  Резервирование критичных компонент ИС. | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы  Наличие регламентированных процедур резервного копирования и восстановления данных. |
| 1.2 | Внедрение и использование работником неучтенного программного обеспечения, в том числе вредоносного. | Применение сертифицированных средств, обеспечивающих невозможность несанкционированной установки пользователем ПО.  Права на установку ПО должен иметь только администратор системы.  Использование сертифицированных средств антивирусной защиты.  Использование для анализа сетевого трафика, электронной почты, защиты серверов антивирусное ПО разных производителей. | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Политика антивирусной защиты; * Инструкция по антивирусной защите; * Инструкция пользователя по безопасной работе в сети Интернет; * Памятка по информационной безопасности пользователя ИС.   Проведение мероприятий по повышению осведомленности пользователей ИС в вопросах защиты информации. |
| 1.3 | Игнорирование работником организационных ограничений (установленных правил) при работе с информационными ресурсами ИС, включая СЗИ. | | |
| 1.3.1 | Нарушение правил хранения и передачи защищаемой информации. | Использование сертифицированных межсетевых экранов. Правила межсетевого экранирования должны разрешать только необходимое для функционирования компонентов информационной системы сетевое взаимодействие.  Мониторинг соблюдения правил хранения и передачи защищаемой информации с использованием специализированных сертифицированных программных средств, в том числе средств DLP (Data Leakage Prevention). | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Памятка по информационной безопасности пользователя ИС. * Процедура предоставления доступа к информационным ресурсам. * Процедура предоставления доступа к внешним сетевым ресурсам. * Инструкция пользователя по безопасной работе в сети Интернет. |
| 1.3.2 | Предоставление работником посторонним лицам возможности доступа к компонентам ИС, а также к самой информации. | Использование сертифицированные средства разграничения доступа. | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы  Проведение периодических мероприятий по повышению осведомленности пользователей ИС в вопросах защиты информации.  Регламентирование правил доступа технического персонала (уборщики, электрики и т.п.) в помещения, в которых находятся компоненты ИС. |
| 1.3.3 | Настройка и конфигурирование пользователем компонент ИС в нарушение нормативных технических документов. | Использование специализированных сертифицированных средств анализа защищенности компонентов ИС.  Использование средств разграничения прав доступа пользователей.  Использовать средства разграничения прав настройки компонентов администраторами ИС. | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны), определяющих порядок настройки и конфигурирования компонентов ИС.  Проведение периодических мероприятий по повышению осведомленности пользователей ИС в вопросах защиты информации. |
| 1.3.4 | Утрата, компрометация пользователем ИС ключевой, парольной и аутентифицирующей информации, любой другой защищаемой информации, а также несообщение о фактах компрометации и утраты такой информации. | Данный тип мер противодействия не применим для рассматриваемой угрозы. | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Политика использования носителей информации и мобильных устройств; * Процедура учета носителей информации и мобильных устройств. * Памятка по информационной безопасности пользователя ИС. * Процедура идентификации, анализа и реагирования на инциденты ИБ; * Процедура расследования инцидентов ИБ.   Проведение периодических мероприятий по повышению осведомленности пользователей ИС в вопросах защиты информации. |
| 1.4 | Сбои в функционировании программного обеспечения ИС. | Мониторинг работоспособности ПО ИС (мониторинг состояния логических серверов: приложений и баз данных)  Использование средств обеспечения отказоустойчивости и балансировки нагрузки.  Использование средств резервного копирования и восстановления. | Разработка документов, определяющие порядок реагирования на сбои ПО и инциденты ИБ. |
| 1.5 | Сбои в функционировании аппаратного обеспечения ИС. | Мониторинг работоспособности аппаратного ИС (мониторинг состояния физических серверов).  «Горячее» резервирование серверов.  «Холодное» резервирование серверов. | Наличие запасных частей и принадлежности (ЗИП) для необходимого количества аппаратных компонентов ИС. |
| 1.6 | Ошибки в проектировании ИС. | Данный тип мер противодействия не применим для рассматриваемой угрозы. | Привлекать для проектирования ИС специализированные организации, обладающие соответствующими лицензиями и опытом проведения подобных работ или привлекать для проектирования ИС собственных специалистов, обладающих необходимыми знаниями, навыками и опытом. |

*Таблица* *9 – Модель защиты информации ИС от угроз, являющихся атаками*

| **№** | **Описание** | **Меры по противодействию** | |
| --- | --- | --- | --- |
| **Технические** | **Организационные** |
| **1** | **Угрозы несанкционированного доступа к информации** | | |
| 1.1 | Изменение параметров загрузки операционной системы серверов (в том числе загрузка ОС с внешних накопителей). | Использование сертифицированных средств защиты информации от НСД.  Использование системы контроля доступа в серверные помещения и к серверному оборудованию. | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы  Регламентация процесса предоставления доступа к серверному оборудованию.  Проведение контроля целостности ОС с использованием сертифицированных СЗИ от НСД.  Отключение и опечатывание неиспользуемых портов ввода/вывода данных. |
| 1.2 | Получение непосредственного доступа к программным компонентам СВТ. | Использование идентификации и аутентификации пользователя при входе в систему.  Ограничение возможности использования съемных носителей.  Использование сертифицированных средств антивирусной защиты.  Регистрация входа/выхода пользователей в систему и из системы, регистрация результата попытки входа. | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы  Разработать и ознакомить под подпись всех пользователей ИС с Памяткой по информационной безопасности пользователя.  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Политика использования носителей информации и мобильных устройств; * Процедура учета носителей информации и мобильных устройств. |
| 1.3 | Кража носителей информации | Использование специализированных сертифицированных средств контроля использования съемных носителей.  Использование системы контроля доступа в серверные помещения | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Политика использования носителей информации и мобильных устройств; * Процедура учета носителей информации и мобильных устройств.   Все носители информации хранить в запираемых шкафах или ящиках стола.  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Процедура идентификации, анализа и реагирования на инциденты ИБ; * Процедура расследования инцидентов ИБ.   Все посетители, попадающие в пределы серверных помещений, должны находиться в них в сопровождении ответственного работника.  Доступ обслуживающего персонала (уборщики, электрики и т.п.) в помещения, в которых находятся компоненты ИС, должен осуществлять под контролем ответственных лиц. |
| 1.4 | Восстановление информации с носителей, вышедших из употребления | Гарантированное уничтожение носителей информации, вышедших из употребления, сертифицированными средствами. | Разработать Процедуру утилизации носителей информации. Процедура должна учитывать особенности утилизации разных типов носителей, а также особенности сервисного обслуживания вычислительной техники. |
| 1.5 | Порча или отключение критичных компонентов ИС | Использование специализированных программных и аппаратных средств обеспечения отказоустойчивости и балансировки нагрузки.  Использование специализированных программно-аппаратных средств резервного копирования и восстановления. | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы  Регламентировать порядок обслуживания компонентов ИС.  Разработать и ознакомить под подпись всех пользователей ИС с Памяткой по информационной безопасности пользователя.  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Процедура идентификации, анализа и реагирования на инциденты ИБ; * Процедура расследования инцидентов ИБ. * Регламентации процедур резервного копирования |
| 1.6 | Несанкционированное копирование конфиденциальной информации на внешние носители. | Использование специализированных сертифицированных программных средств разграничения доступа пользователей к портам USB, CD/DVD и т.п.  Мониторинг соблюдения правил хранения и передачи защищаемой информации с использованием специализированных сертифицированных программных средств, в том числе средств DLP (Data Leakage Prevention). | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Политика использования носителей информации и мобильных устройств; * Процедура учета носителей информации и мобильных устройств. |
| 2 | ***Угрозы, реализуемые с использованием протоколов межсетевого взаимодействия*** | | |
| 2.1 | Сканирование сети | Использование сертифицированных межсетевых экранов (правила межсетевого экранирования должны разрешать только необходимое для функционирования компонентов ИС сетевое взаимодействие).  Использование сертифицированных средств обнаружения компьютерных атак, выявляющие попытки сканирования сети.  Использование сертифицированных средств анализа защищенности. | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Инструкция администратора информационной безопасности; * Процедура идентификации, анализа и реагирования на инциденты ИБ; * Процедура расследования инцидентов ИБ. |
| 2.2 | Подбор злоумышленником аутентифицирующей информации администраторов ИС | Ограничение количества неудачных попыток входа в систему. | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Политика парольной защиты; * Процедура идентификации, анализа и реагирования на инциденты ИБ; * Процедура расследования инцидентов ИБ. |
| 2.3 | Проведение атак типа «отказ в обслуживании» на каналы связи | Использование сертифицированных межсетевых экранов и средств обнаружения/ предотвращения вторжений.  Использование сертифицированных средств анализа защищенности. | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Инструкция администратора информационной безопасности; * Процедура идентификации, анализа и реагирования на инциденты ИБ; * Процедура расследования инцидентов ИБ. |
| 2.4 | Проведение компьютерных атак на СВТ с целью получения несанкционированного доступа к программной среде СВТ | Функционирование закрытой части ИС в защищенном контуре. При этом доступ к закрытой части ИС имеют только сотрудники, учетные записи которых зарегистрированы в корпоративном MS AD и ИС.  Использование сертифицированных межсетевых экранов.  Использование специализированных сертифицированных программных и/или программно-аппаратных средств предотвращения компьютерных атак.  Использование сертифицированного антивирусного ПО разных производителей  Использовать специализированных сертифицированных программных и/или программно-аппаратных средств защиты от НСД.  Использование специализированных средств анализа защищенности. | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы  Периодический анализ защищенности компонентов ИС с использованием специализированных программных средств.  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Инструкция администратора информационной безопасности; * Процедура идентификации, анализа и реагирования на инциденты ИБ; * Процедура расследования инцидентов ИБ. |
| 2.5 | Размещение защищаемой информации на незащищенных или не предназначенных для этих целей ресурсах ИС | Использование сертифицированных межсетевых экранов (правила межсетевого экранирования должны разрешать только необходимое для функционирования компонентов ИС сетевое взаимодействие). | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Инструкция администратора информационной безопасности. * Инструкция по работе с коммерческой тайной. * Инструкция по работе с персональными данными. * Инструкция по работе со служебной информацией ограниченного распространения. * Процедура идентификации, анализа и реагирования на инциденты ИБ. * Процедура расследования инцидентов ИБ. |
| 2.6 | Передача защищаемой информации по сети за пределы КЗ | Использование фильтрации сетевого трафика в зависимости от передаваемой информации.  Использование специализированных сертифицированных средств предотвращения утечки информации | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Процедура идентификации, анализа и реагирования на инциденты ИБ. * Процедура расследования инцидентов ИБ. |
| 2.7. | Модификация защищаемой информации при ее передаче по каналам связи | Осуществление шифрования данных при их передаче за пределы КЗ с использованием сертифицированных ФСБ России СКЗИ. | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Инструкция администратора информационной безопасности. * Процедура идентификации, анализа и реагирования на инциденты ИБ. * Процедура расследования инцидентов ИБ. |
| 3 | ***Угрозы программно-математических воздействий*** | | |
| 3.1 | Внедрение в ПО вредоносных программ (вирусов, троянов, backdoor и т.п.) | Использование сертифицированных средств антивирусной защиты.  Использование для анализа сетевого трафика, электронной почты и защиты серверов антивирусного ПО разных производителей.  Осуществление доступа к сети Интернет с использованием терминальных решений. | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Политика антивирусной защиты. * Инструкция по антивирусной защите. * Инструкция пользователя по безопасной работе с Интернет. * Процедура идентификации, анализа и реагирования на инциденты ИБ. * Процедура расследования инцидентов ИБ. |
| **4** | **Угроз преднамеренных действий нарушителей** | | |
| 4.1. | Выявление сведений о структуре ИС, применяемых СВТ, средствах и подсистеме защиты обрабатываемой информации (использование методов «социальной инженерии») | Данный тип мер противодействия не применим для рассматриваемой угрозы | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы  Ознакомление под подпись всех пользователей ИС с Памяткой по информационной безопасности пользователя  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Процедура идентификации, анализа и реагирования на инциденты ИБ; * Процедура расследования инцидентов ИБ. |
| 4.2. | Публикация информации от имени другого пользователя ИС | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа  Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы  Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы  Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)  Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы  Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу  Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы  Ознакомление под подпись всех пользователей ИС с Памяткой по информационной безопасности пользователя  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Процедура идентификации, анализа и реагирования на инциденты ИБ;   Процедура расследования инцидентов ИБ. |
| 4.3. | Отказ от авторства передаваемой/ принимаемой информации | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа  Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы  Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы  Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)  Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы  Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу  Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации | Наличие на предприятии службы информационной безопасности как выделенной структурной единицы  Ознакомление под подпись всех пользователей ИС с Памяткой по информационной безопасности пользователя  Использование на предприятии единых регламентирующих документов (если их нет, должны быть разработаны):   * Процедура идентификации, анализа и реагирования на инциденты ИБ;   Процедура расследования инцидентов ИБ. |

# 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.