|  |  |
| --- | --- |
| УТВЕРЖДАЮ  Генеральный директор ГК Астра  \_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_ /  «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_г. |  |

**Модель угроз безопасности информации защищённой автоматизированной информационной системы ГК Астра**

Москва 2023

СОДЕРЖАНИЕ

[1 ОБЩИЕ ПОЛОЖЕНИЯ 5](#_Toc148008871)

[1.1 Назначение и область действия документа 5](#_Toc148008872)

[1.2 Нормативные правовые акты, методические документы, национальные стандарты, используемые для оценки угроз безопасности информации и разработки модели угроз 6](#_Toc148008873)

[1.3 Наименование обладателя информации, заказчика, оператора систем и сетей 7](#_Toc148008874)

[1.4 Подразделения, должностные лица, ответственные за обеспечение защиты информации (безопасности) систем и сетей 7](#_Toc148008875)

[1.5 Наименование организации, привлекаемой для разработки модели угроз безопасности информации (при наличии) 7](#_Toc148008876)

[2 ОПИСАНИЕ СИСТЕМ И СЕТЕЙ И ИХ ХАРАКТЕРИСТИКА КАК ОБЪЕКТОВ ЗАЩИТЫ 8](#_Toc148008877)

[2.1. Наименование систем и сетей, для которых разработана модель угроз безопасности информации 8](#_Toc148008878)

[2.2. Класс защищенности, категория значимости систем и сетей, уровень защищенности персональных данных 8](#_Toc148008879)

[2.3. Нормативные правовые акты Российской Федерации, в соответствии с которыми создаются и (или) функционируют системы и сети 8](#_Toc148008880)

[2.4. Назначение, задачи (функции) систем и сетей, состав обрабатываемой информации и ее правовой режим 8](#_Toc148008881)

[2.5 Основные процессы обладателя информации, для обеспечения которых создаются (функционируют) системы и сеты 10](#_Toc148008882)

[2.6 Описание групп внешних и внутренних пользователей систем и сетей, уровней их полномочий и типов доступа (в состав групп пользователей включается все пользователи, для которых требуется авторизация при доступе к информационным ресурсам, и пользователи, для которых не требуется авторизация) 11](#_Toc148008883)

[2.7 Описание функционирования систем и сетей на базе информативно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры: 11](#_Toc148008884)

[2.8 Описание модели предоставления вычислительных услуг, распределения ответственности за защиту информации между обладателями информации, оператором и поставщиком вычислительных услуг 12](#_Toc148008885)

[2.9 Описание условий использования информационно-телекоммуникационной инфраструктуры обработки данных или облачной инфраструктуры поставщика услуг (при наличии) 12](#_Toc148008886)

[4 ВОЗМОЖНЫЕ НЕГАТИВНЫЕ ПОСЛЕДСТВИЯ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. ВОЗМОЖНЫЕ ОБЪЕКТЫ ВОЗДЕЙСТВИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. ИСТОЧНИКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. СПОСОБЫ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ 13](#_Toc148008887)

[5 АКТУАЛЬНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИ 17](#_Toc148008888)

**ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ**

|  |  |  |
| --- | --- | --- |
| АИС | – | Автоматизированная информационная система |
| БД | – | База данных |
| ИСПДн | – | Информационная система персональных данных |
| НСД | – | Несанкционированный доступ |
| ПДн | – | Персональные данные |
| ФГБУ | – | Федеральное государственное бюджетное учреждение |

# 1 ОБЩИЕ ПОЛОЖЕНИЯ

# 1.1 Назначение Модели угроз

Разработка модели угроз безопасности информации выполняется для определения актуальных угроз безопасности защищаемой информации, обрабатываемой в АИС ГК Астра.

Результаты определения актуальных угроз безопасности защищаемой информации предназначены для формирования обоснованных требований к составу и содержанию мер по обеспечению информационной безопасности АИС ГК Астра.

# 1.2 Нормативные правовые акты, методические документы, национальные стандарты, используемые для оценки угроз безопасности информации и разработки модели угроз

Определение угроз безопасности информации осуществлялось на основании технических требований, действующего законодательства Российской Федерации. В перечень используемых нормативных источников входят, но не ограничиваются ими:

– Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных»;

– Постановление Правительства Российской Федерации от 01 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Приказ ФСТЭК России от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Методика оценки угроз безопасности информации ФСТЭК России, утвержденная ФСТЭК России 5 февраля 2021 г

– «Требования к системам обнаружения вторжений» (утвержден приказом ФСТЭК России от 06.12.2011 N 638. ДСП);

– «Требования к средствам антивирусной защиты» (утвержден приказом ФСТЭК России от 20.03.2012 N 28. ДСП);

– «Требования к средствам доверенной загрузки» (утвержден приказом ФСТЭК России от 27.09.2013 N 119. ДСП);

– «Требования к межсетевым экранам» (утвержден приказом ФСТЭК России от 09.02.2016 N 9. ДСП);

– «Требованиям безопасности информации к операционным системам» (утвержден приказом ФСТЭК России от 19.08.2016 N 119. ДСП);

– «Требования к средствам контроля съёмных машинных носителей информации» (утвержден приказом ФСТЭК России от 28.07.2014 N 87. ДСП);

– Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий (введён в действие приказом Гостехкомиссии России от 19 июня 2002 г. N 187).

1.3 Область применения настоящей Модели угроз

Областью применения процесса определения угроз безопасности информации является совокупность информационных и программно-аппаратных элементов, а также информационных технологий, применяемых при обработке информации в АИС ГК Астра.

Элементами АИС ГК Астра являются:

– информация заказчика, как совокупность информации и её носителей, используемых в АИС ГК Астра;

– информационные технологии, применяемые при обработке информации;

– технологические средства, осуществляющие обработку информации (средства вычислительной техники, информационно-вычислительные комплексы сети, средства и системы хранения, передачи, приема и обработки информации);

– программные средства инфраструктурного уровня (в том числе операционные системы технических средств АИС ГК Астра);

– средства защиты информации;

– подсистемы и сервисы, образуемые на основе технических и программных средств, средства защиты информации АИС ГК Астра (в том числе инфраструктурные подсистемы, инфраструктурные сервисы, подсистемы информационной безопасности).

1.4 Наименование обладателя информации, заказчика, оператора систем и сетей

Обладателем информации, заказчиком и оператором систем и сетей является ГК Астра.

1.5 Подразделения, должностные лица, ответственные за обеспечение защиты информации (безопасности) систем и сетей

Ответственность за обеспечение защиты информации (безопасности) систем и сетей возлагается на:

– руководителей подразделений ГК Астра;

– работников, ответственных за администрирование сегментов информационной телекоммуникационной системы ГК Астра;

– работников, выполняющих следующие функции: администраторов информационных систем, администраторов локальной вычислительной сети, администраторов по обеспечению безопасности информации.

1.6 Наименование организации, привлекаемой для разработки модели угроз безопасности информации (при наличии)

Отсутствует, разработка произведена собственными силами.

# 2 ОПИСАНИЕ СИСТЕМ И СЕТЕЙ И ИХ ХАРАКТЕРИСТИКА КАК ОБЪЕКТОВ ЗАЩИТЫ

# 2.1. Наименование систем и сетей, для которых разработана модель угроз безопасности информации

– объект 1 – информационная система персональных данных ГК Астра;

– объект 2 – ЛВС, в рамках которой работники обеспечивают обмен информацией;

– объект 3 – сервер, на котором хранятся БД ИСПДн, АИС ГК Астра.

# 2.2. Класс защищенности, категория значимости систем и сетей, уровень защищенности персональных данных

Уровень защищенности ИСПДн АИС ГК Астра – первый

# 2.3. Нормативные правовые акты Российской Федерации, в соответствии с которыми создаются и (или) функционируют системы и сети

АИС ГК Астра разработана в соответствии с положениями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», а также иными подзаконными нормативно-правовыми актами в сфере персональных данных.

# 2.4. Назначение, задачи (функции) систем и сетей, состав обрабатываемой информации и ее правовой режим

ИСПДн предназначена для обработки информации о сотрудниках и специалистах с целью обеспечения безопасности от несанкционированного доступа на объект посторонних людей, порчи имущества, наблюдение за поведением персонала, а также хранение всей информации на сервере.

Персональные данные специалистов в АСИ ГК Астра обрабатываются с целью:

– организации рабочего процесса;

– защиты специалистов, и их прав, интересов, имущества от неблагоприятных воздействий;

– обеспечения защиты от несанкционированного проникновения на территорию посторонних лиц и транспортных средств;

– предупреждения, устранения причин (последствий) деятельности, приводящей к порче имущества ГК Астра;

– предоставления информации по запросам соответствующих служб и государственных органов в случаях, предусмотренных действующим законодательством.

Персональные данные специалистов включают в себя:

– фамилию, имя, отчество специалиста;

– серию и номер документа, удостоверяющего личность специалиста, кем и когда выдан;

– дату рождения специалиста;

– адрес проживания специалиста;

– реквизиты ИНН специалиста;

– реквизиты страхового номера Индивидуального лицевого счета в Пенсионном фонде РФ специалиста;

– сведения о доходах специалиста (номер банковской карты, номер лицевого счета, размер оклада, размер надбавок, премий);

– сведения о начислениях специалиста.

Персональные данные сотрудников ГК Астра обрабатываются с целью:

– обеспечения защиты прав и обязанностей сотрудников;

– обеспечения защита от несанкционированного проникновения на территорию посторонних лиц и транспортных средств;

– осуществления трудовых отношений;

– передачи данных в уполномоченные органы (ФНС, ФСС, ПФР);

– ведения расчётов заработной платы и надбавок;

– осуществления банковских операций.

Персональные данные сотрудников ГК Астра включает в себя:

– фамилию, имя, отчество сотрудника;

– серию и номер документа, удостоверяющего личность работника, кем и когда выдан;

– дату рождения сотрудника;

– адрес проживания сотрудника;

– реквизиты ИНН сотрудника;

– реквизиты страхового номера Индивидуального лицевого счета в Пенсионном фонде РФ сотрудника;

– сведения о доходах сотрудника (номер банковской карты, номер лицевого счета, размер оклада, размер надбавок, премий);

– сведения о начислениях сотрудников.

Правовые основания обработки персональных данных: Трудовой кодекс РФ, Налоговый кодекс, ФЗ «О бухгалтерском учете», лицензия на осуществление банковских операций, согласие на обработку персональных данных.

# 2.5 Основные процессы обладателя информации, для обеспечения которых создаются (функционируют) системы и сеты

Такими процессами являются обеспечение физической безопасности находящихся на объекте сотрудников и специалистов, а также хранение, обработка и защита персональных данных.

# 2.6 Описание групп внешних и внутренних пользователей систем и сетей, уровней их полномочий и типов доступа (в состав групп пользователей включается все пользователи, для которых требуется авторизация при доступе к информационным ресурсам, и пользователи, для которых не требуется авторизация)

Таблица 1 – Описание групп пользователей

|  |  |  |
| --- | --- | --- |
| **Типовая роль** | **Уровень доступа к ПДн** | **Разрешенные действия по отношению к ПДн** |
| Администратор ИСПДн | Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн, обладает полной информацией о технических средствах и конфигурации ИСПДн, имеет доступ ко всем техническим средствам обработки информации и данных ИСПДн, обладает правами конфигурирования и административной настройки технических средств ИСПДн | Систематизация, хранение, уточнение, использование, обезличивание, блокировка, уничтожение |
| Пользователи ИСПДн | Обладают полной информацией о системном и прикладном программном обеспечении ИСПДн | Сбор, систематизация, хранение, уточнение, использование, распространение, обезличивание, блокирование, уничтожение |
| Лица, обладающие возможностью доступа к системе передачи данных | Обладают информацией о системном и прикладном программном обеспечении ИСПДн | Уточнение, использование |
| Пользователи, являющиеся внешними по отношению к ИСПДн | Информация относящееся к самому субъекту. | Уточнение |
| Обслуживающий персонал | Отсутствует | Отсутствует |

# 2.7 Описание функционирования систем и сетей на базе информативно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры:

Не реализовано.

# 2.8 Описание модели предоставления вычислительных услуг, распределения ответственности за защиту информации между обладателями информации, оператором и поставщиком вычислительных услуг

Не реализовано.

# 2.9 Описание условий использования информационно-телекоммуникационной инфраструктуры обработки данных или облачной инфраструктуры поставщика услуг (при наличии)

Не реализовано.

# 3 ВОЗМОЖНЫЕ НЕГАТИВНЫЕ ПОСЛЕДСТВИЯ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. ВОЗМОЖНЫЕ ОБЪЕКТЫ ВОЗДЕЙСТВИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. ИСТОЧНИКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. СПОСОБЫ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Таблица 2 – Описание групп внешних и внутренних нарушителя объекта

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Объект** | **Назначение объекта** | **Вид/категория нарушителя/возможности нарушителя** | **Виды воздействия/негативные последствия** | **Соотнесение с угрозами** | **Цели реализации угроз** | **Описание способов реализации угроз/ описание интерфейсов объектов воздействия** |
| Разработчики ИСПДн | Предназначен для обработки информации о сотрудниках учреждения с целью учета рабочего времени, начисления заработной платы, формирования отчётности в контролирующие органы | Имеет возможность приобретать информацию об уязвимостях, размещаемую на специализированных платных ресурсах (биржах уязвимостей)  Имеет возможность приобретать дорогостоящие средства и инструменты для реализации угроз, размещаемые на специализированных платных ресурсах (биржах уязвимостей)  Имеет возможность самостоятельно разрабатывать средства, необходимые для реализации угроз (атак), реализовывать угрозы с использованием данных средств | Вид воздействия: Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных.  Негативные последствия: Подмена данных работников организации, платежных реквизитов, отчетности. | Возможно, при реализации угроз | Непреднамеренны, неосторожные или неквалифицированные действия | Внедрение вредоносного программного обеспечения/ Доступ через локальную вычислительную сеть организации Использование уязвимостей конфигурации системы управления доступом к АРМ пользователя/ Съемные машинные носители информации, подключаемые к АРМ пользователя |
| Специалист | Имеют право доступа к локальным ИСПДн для выполнения своих должностных обязанностей. | Располагает именами и паролями зарегистрированных пользователей ИСПДн  Изменяет конфигурацию технических средств обработки ПДн, вносит программно-аппаратные закладки в ИСПДн и обеспечивать съём информации, используя непосредственное подключение к техническим средствам обработки информации | Вид воздействия: Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных Негативные последствия: Подмена данных работников организации, платежных реквизитов, отчетности. | Возможно, при реализации угроз | Непреднамеренны, неосторожные или неквалифицированные действия | Внедрение вредоносного программного обеспечения (доступ через локальную вычислительную сеть организации)  Использование уязвимостей конфигурации системы управления (съемные машинные носители информации, подключаемые к АРМ пользователя) |
| Системный администратор | Выполняет конфигурирование и управление программным обеспечением и оборудованием, включая оборудование, отвечающее за безопасность защищаемого объекта (средства мониторинга, резервного копирования, антивирусного контроля, защиты от несанкционированного доступа) | Обладает полной информацией о системном, специальном и прикладном ПО, используемом в ИСПДн  Обладает полной информацией о конфигурации ИСПДн (имеет доступ ко всем ИСПДн и данным)  Обладает правами конфигурирования и административной настройки ИСПДн | Вид воздействия: утечка (перехват) конфиденциальной информации или отдельных данных  Негативные последствия: разглашение персональных данных. | Возможно, при реализации угроз | Месть, непреднамеренные, неосторожные или неквалифицированные действия | Использование уязвимостей конфигурации системы управления доступом к АРМ пользователя (съёмные машинные носители информации, подключаемые к АРМ пользователя)  Использование уязвимостей конфигурации системы управления доступом к АРМ пользователя (сетевые интерфейсы коммутатора сети, где расположен веб-сервер) |

Таблица 3 – Оценка целей реализации нарушителями угроз безопасности информации в зависимости от возможных негативных последствий и видов ущерба от их реализации

|  |  |  |
| --- | --- | --- |
| **Виды нарушителя** | **Категория нарушителя** | **Возможные цели реализации угроз безопасности информации** |
| Отдельные физические лица (хакеры) | Внешний | Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса) |
| Конкурирующие организации | Внешний | Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды |
| Разработчики программных, программноаппаратных средств | Внутренний | Внедрение дополнительных функциональных возможностей в программные или программноаппаратные средства на этапе разработки. Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия |
| Лица, обеспечивающие поставку программных, программноаппаратных средств, обеспечивающих систем | Внешний | Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия.  Получение конкурентных преимуществ |
| Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ | Внутренний | Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия.  Получение конкурентных преимуществ |
| Авторизованные пользователи систем и сетей | Внутренний | Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия |
| Бывшие работники (пользователи) | Внешний | Получение финансовой или иной материальной выгоды. Месть за ранее совершенные действия |

# 5 АКТУАЛЬНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИ

Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для ПДн.

Актуальность угрозы определяется следующими параметрами:

- уровень исходной защищенности ИСПДн;

- частота (вероятность) реализации рассматриваемой угрозы.

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн. Характеристики ИСПДн ГК Астра приведены в таблице 4.

Таблица 4 – Показатели исходной защищенности ИСПДн ГК Астра

|  |  |  |  |
| --- | --- | --- | --- |
| **Технические и эксплуатационные характеристики ИСПДн** | **Уровень защищенности** | | |
| **Высокий** | **Средний** | **Низкий** |
| **1. По территориальному размещению:** |  | + |  |
| распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом; | – | – | – |
| городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка); | – | – | – |
| корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации; | – | – | – |
| **локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;** | – | + | – |
| локальная ИСПДн, развернутая в пределах одного здания | – | – | – |
| **2. По наличию соединения с сетями общего пользования:** |  | + |  |
| ИСПДн, имеющая многоточечный выход в сеть общего пользования; | – | – | – |
| **ИСПДн, имеющая одноточечный выход в сеть общего пользования;** | – | + | – |
| ИСПДн, физически отделенная от сети общего пользования | – | – | – |
| **3. По встроенным (легальным) операциям с записями баз персональных данных:** |  |  | + |
| **чтение, поиск;** | – | – | + |
| **запись, удаление, сортировка;** | – | + | – |
| **модификация, передача** | – | – | + |
| **4.По разграничению доступа к персональным данным:** |  | + |  |
| **ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;** | – | + | – |
| **ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;** | – | + | – |
| ИСПДн с открытым доступом | – | – | – |
| **5. По наличию соединений с другими базами ПДн иных ИСПДн:** |  | + |  |
| **интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн);** | – | + | – |
| ИСПДн, в которой используется  одна база ПДн, принадлежащая организации – владельцу данной ИСПДн | – | – | – |
| **6. По уровню обобщения (обезличивания) ПДн:** |  |  | + |
| ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.); | – | – | – |
| **ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;** | – | – | + |
| ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн) | – | – | – |
| **7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:** | + |  |  |
| ИСПДн, предоставляющая всю базу данных с ПДн; | – | – | – |
| ИСПДн, предоставляющая часть ПДн; | – | – | – |
| **ИСПДн, не предоставляющая никакой информации.** | + | – | – |

Значению уровня защищенности «Высокий» соответствуют 2 характеристики, значению уровня «Средний» - 5 характеристики, значению уровня «Низкий» - 1 характеристика. Таким образом, числовой коэффициент исходной защищенности ИСПДн ГК Астра Y1 соответствует значению 5 (средняя степень исходной защищенности).

Для каждой угрозы определяется вероятность реализации угрозы Y2 и соответствующий коэффициент:

0 - для маловероятной угрозы;

2 - для низкой вероятности угрозы;

5 - для средней вероятности угрозы;

10 - для высокой вероятности угрозы.

С учётом этого реализуемость каждой угрозы Y рассчитывается по формуле: Y = (Y1+Y2)/20.

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

если 0 ≤ Y ≤ 0.3, то возможность реализации угрозы признается низкой;

если 0.3 < Y ≤ 0.6, то возможность реализации угрозы признается средней;

если 0.6 < Y ≤ 0.8, то возможность реализации угрозы признается высокой;

если Y < 0.8, то возможность реализации угрозы признается очень высокой.

Далее оценивается опасность каждой угрозы. При оценке опасности на основе опроса экспертов определяется вербальный показатель опасности для рассматриваемой ИСПДн.

Этот показатель имеет три значения:

1) низкая опасность - если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

2) средняя опасность - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

3) высокая опасность - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Затем осуществляется выбор из общего (предварительного) перечня угроз безопасности тех, которые относятся к актуальным для данной ИСПДн, в соответствии с правилами, приведенными в таблице 5.

Таблица 5 – Правила отнесения угрозы безопасности ПДн к актуальной

|  |  |  |  |
| --- | --- | --- | --- |
| **Возможность реализации угрозы** | **Показатель опасности угрозы** | | |
| Низкая | Средняя | Высокая |
| Низкая | неактуальна | неактуальная | актуальная |
| Средняя | неактуальная | актуальная | актуальная |
| Высокая | актуальная | актуальная | актуальная |
| Очень высокая | актуальная | актуальная | актуальная |

Состав угроз определен следующим образом. На основе «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных» установлена типовая модель угроз безопасности, актуальная для ГК Астра: Типовая модель угроз безопасности персональных данных, обрабатываемых в распределенных информационных системах персональных данных, имеющих подключение к сетям связи общего пользования и(или) сетям международного информационного обмена.

Для данной типовой модели возможна реализация следующих угроз безопасности ПДн (табл. 6).

Таблица 6 – Таблица угроз и их характеристики

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Наименование угрозы** | **Вероятность (Y2)** | **Реализуемость (Y)** | **Опасность** | **Актуальность** |
| *Угрозы утечки информации по техническим каналам* | | | | |
| Угрозы утечки акустической (речевой) информации | маловероятно (0) | низкая (0.25) | низкая | неактуальная |
| Угрозы утечки видовой информации | маловероятно (0) | низкая (0.25) | низкая | неактуальная |
| Угрозы утечки информации по каналу ПЭМИН | маловероятно (0) | низкая (0.25) | низкая | неактуальная |
| *Угрозы НСД к ПДн непосредственно в ИСПДн* | | | | |
| Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой | маловероятно (0) | низкая (0.25) | средняя | неактуальная |
| Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование и т.п.) операционной системы или какой-либо прикладной программы, с применением специально созданных для выполнения НСД программ | маловероятно (0) | низкая (0.25) | средняя | неактуальная |
| Угрозы внедрения вредоносных программ | средняя вероятность (5) | средняя (0.5) | низкая | неактуальная |
| *Сетевые угрозы* | | | | |
| Угрозы "Анализа сетевого трафика" с перехватом передаваемой по сети информации | низкая вероятность (2) | средняя (0.35) | средняя | актуальная |
| Угрозы выявления паролей | низкая вероятность (2) | средняя (0.35) | средняя | актуальная |
| Угрозы удаленного запуска приложений | низкая вероятность (2) | средняя (0.35) | средняя | актуальная |
| Угрозы внедрения по сети вредоносных программ | низкая вероятность (2) | средняя (0.35) | низкая | неактуальная |
| *Угрозы из внешних сетей* | | | | |
| Угрозы “Анализа сетевого трафика” с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации | низкая вероятность (2) | средняя (0.35) | средняя | актуальная |
| Угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др. | маловероятно (0) | низкая (0.25) | низкая | неактуальная |
| Угрозы выявления паролей | низкая вероятность (2) | средняя (0.35) | средняя | актуальная |
| Угрозы получения НСД путем подмены доверенного объекта | маловероятно (0) | низкая (0.25) | низкая | неактуальная |
| Угрозы типа "Отказ в обслуживании" | низкая вероятность (2) | средняя (0.35) | средняя | актуальная |
| Угрозы удаленного запуска приложений | маловероятно (0) | низкая (0.25) | низкая | неактуальная |
| Угрозы внедрения по сети вредоносных программ | средняя вероятность (5) | средняя (0.5) | средняя | актуальная |

По результатам, ИСПДн ГК Астра соответствует среднему уровню защищенности.