|  |  |
| --- | --- |
| УТВЕРЖДАЮ  Руководитель  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 202\_г. |  |

**Модель угроз безопасности информации защищённой автоматизированной информационной системы ФГБУ «НПП «ГАММА»**

г. Москва

2023 г.

СОДЕРЖАНИЕ

[1 ОБЩИЕ ПОЛОЖЕНИЯ 5](#_Toc148365115)

[1.1 Назначение и область действия документа 5](#_Toc148365116)

[1.2 Нормативные правовые акты, методические документы, национальные стандарты, используемые для оценки угроз безопасности информации и разработки модели угроз 5](#_Toc148365117)

[1.3 Наименование обладателя информации, заказчика, оператора систем и сетей 6](#_Toc148365118)

[1.4 Подразделения, должностные лица, ответственные за обеспечение защиты информации (безопасности) систем и сетей 6](#_Toc148365119)

[1.5 Наименование организации, привлекаемой для разработки модели угроз безопасности информации (при наличии) 6](#_Toc148365120)

[2 ОПИСАНИЕ СИСТЕМ И СЕТЕЙ И ИХ ХАРАКТЕРИСТИКА КАК ОБЪЕКТОВ ЗАЩИТЫ 7](#_Toc148365121)

[2.1. Наименование систем и сетей, для которых разработана модель угроз безопасности информации 7](#_Toc148365122)

[2.2. Класс защищенности, категория значимости систем и сетей, уровень защищенности персональных данных 7](#_Toc148365123)

[2.3. Нормативные правовые акты Российской Федерации, в соответствии с которыми создаются и (или) функционируют системы и сети 7](#_Toc148365124)

[2.4. Назначение, задачи (функции) систем и сетей, состав обрабатываемой информации и ее правовой режим 8](#_Toc148365125)

[2.5 Основные процессы обладателя информации, для обеспечения которых создаются (функционируют) системы и сеты 9](#_Toc148365126)

[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) 10](#_Toc148365127)

[2.7 Описание функционирования систем и сетей на базе информативно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры: 10](#_Toc148365128)

[2.8 Описание модели предоставления вычислительных услуг, распределения ответственности за защиту информации между обладателями информации, оператором и поставщиком вычислительных услуг 10](#_Toc148365129)

[Не реализовано. 10](#_Toc148365130)

[2.9 Описание условий использования информационно-телекоммуникационной инфраструктуры обработки данных или облачной инфраструктуры поставщика услуг (при наличии) 11](#_Toc148365131)

[3 ИСТОЧНИКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. СПОСОБЫ 12](#_Toc148365132)

[РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОТИ ИНФОРМАЦИИ 12](#_Toc148365133)

[4 АКТУАЛЬНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИ 14](#_Toc148365134)

**ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ**

|  |  |  |
| --- | --- | --- |
| АИС | – | Автоматизированная информационная система |
| БД | – | База данных |
| ИСПДн | – | Информационная система персональных данных |
| ФГБУ | – | Федеральное государственное бюджетное учреждение |
| НИЦ | – | Национальный исследовательский центр |
| НСД | – | Несанкционированный доступ |
| ОС | – | Операционная система |
| ПДн | – | Персональные данные |
| ПО | – | Программное обеспечение |

# 1 ОБЩИЕ ПОЛОЖЕНИЯ

# 1.1 Назначение и область действия документа

Разработка модели угроз безопасности информации выполняется для определения актуальных угроз безопасности защищаемой информации, обрабатываемой в ФГБУ «НПП «ГАММА».

Результаты определения актуальных угроз безопасности защищаемой информации предназначены для формирования обоснованных требований к составу и содержанию мер по обеспечению информационной безопасности ФГБУ «НПП «ГАММА».

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

Определение нарушителей и угроз безопасности персональных данных при их обработке и последующее формирование на их основе модели угроз и

нарушителей является одним из необходимых мероприятий по обеспечению

безопасности в информационных системах:

– 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»;

– 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»;

− Методические рекомендации по обеспечению информационной

безопасности.

– 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»;

1.3 Наименование обладателя информации, заказчика, оператора систем и сетей

Заказчиком и оператором систем и сетей является ФГБУ «НПП «ГАММА».

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

Департаменты, отвечающие за обеспечение безопасности информации выступают:

- Руководитель направления системного администрирования. В задачи данного департамента входит обслуживание и администрирование средств информационной безопасности.

- Отдел информационной безопасности (ИБ). В задачи данного департамента входит анализирование средств информационной безопасности.

1.5 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 ФГБУ «НПП «ГАММА»;

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

– объект 3 – сервер, на котором хранятся БД ИСПДн, ФГБУ «НПП «ГАММА».

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

Класс защищенности: Класс защищенности систем и сетей определяет

уровень и глубину мер безопасности, которые должны быть применены к

информационным ресурсам. В России классы защищенности могут определяться согласно ГОСТ Р ИСО/МЭК 27001-2012 и другим нормативам.

Обычно они имеют следующие обозначения:

- КС1 (критический класс защищенности).

- КС2 (высокий класс защищенности).

- КС3 (средний класс защищенности).

- КС4 (низкий класс защищенности).

Уровень защищенности ИСПДн ФГБУ «НПП «ГАММА» – первый.

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

Настоящая Модель угроз разработана в соответствии с положениями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

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

ИСПДн ФГБУ «НПП «ГАММА» предназначена для обработки, хранения и защиты персональных данных сотрудников, клиентов, поставщиков и других физических лиц, связанных с деятельностью предприятия.

В ИСПДн ФГБУ «НПП «ГАММА» могут обрабатываться следующие персональные данные:

Персональные данные сотрудников ФГБУ «НПП «ГАММА» 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 ФГБУ «НПП «ГАММА» 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.

Правовой режим информации определяется законодательством о защите персональных данных и включает в себя требования к сбору, обработке, хранению и передаче персональных данных.

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

Заказчик ФГБУ «НПП «ГАММА» должен регулярно проводить следующие процессы для обеспечения безопасности информации в инфраструктуре:

* Сбор событий информационной безопасности;
* Обучение сотрудников**;**
* Реагирование на инциденты информационной безопасности;
* Соблюдение законодательства РФ.

# 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 ИСПДн** | **Разрешенные действия к ИСПДн** |
| Администраторы систем и сетей | Обладают полной информацией о системном и прикладном программном обеспечении | Полный доступ к управлению, настройкам и обслуживаниям информационных систем и сетей  предприятия. полный доступ для администрирования |
| Финансовый отдел (бухгалтерия) | Обладают доступом к бухгалтерской информации, финансовым данным. | Доступ к отчетам, договорам компании |
| Специалисты информационной безопасности | Контроль событий ИБ и контроль доступа | Уточнение, использование |
| Заказчики | Отсутствует | Предоставление Пдн |

# 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 ИСТОЧНИКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. СПОСОБЫ

# РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОТИ ИНФОРМАЦИИ

Таблица 3 – Возможные цели реализации угроз безопасности информации нарушителями

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ Вида** | **Отдел** | **Назначение** | **Категория нарушителя** | **Цели реализации угроз** | **Описание способов реализации угроз (описание интерфейсов объектов воздействия)** |
| 1 | Разработчики | Предназначен для разработки средств информационной безопасности для коммерческих и не коммерческих целей. | Внутренний/Внешний | Неосторожность, безалаберность, получение вознаграждения | 1. Внедрение вредоносного программного обеспечения. 2. Использование уязвимостей для получения конфиденциальной информации. |
| 2 | Сотрудники | Имеют право доступа к локальным для выполнения своих должностных обязанностей | Внутренний | Получение финансовой или иной материальной выгоды. Непреднамеренные,  неосторожные или неквалифицированные действия. Получение  конкурентных преимуществ | 1. Внедрение вредоносного программного обеспечения. 2. Использование уязвимостей для получения конфиденциальной информации. |
| 3 | Системный администратор | Выполняет конфигурирование и управление программным обеспечением и оборудованием, включая оборудование, отвечающее за безопасность защищаемого объекта | Внутренний | Получение финансовой выгоды. Финансовые и репутационные убытки для компании | 1. Использование уязвимостей конфигурации системы управления доступом к АРМ пользователя   2. Использование уязвимостей конфигурации системы управления доступом к АРМ пользователя |

Таблица 4 – Оценка целей реализации нарушителями угроз безопасности информации в зависимости от возможных негативных последствий и видов ущерба от их реализации

|  |  |  |
| --- | --- | --- |
| **Виды нарушителей** | **Возможные цели реализации угроз безопасности информации** | **Соответствие цели видам риска (ущерба) и возможным негативным последствиям** |
| Разработчики | + | У2 (утечка коммерческой тайны; причинение  имущественного ущерба; уничтожение данных) |
| Сотрудники | + | У2 (утечка коммерческой тайны; причинение  имущественного ущерба; уничтожение данных) |
| Системный администратор | + | У2 (утечка коммерческой тайны; причинение  имущественного ущерба; уничтожение данных) |

# 4 АКТУАЛЬНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИ

Актуальной угрозой может считаться событие, которое 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 ФГБУ «НПП «ГАММА» приведены в таблице 5.

Таблица 5 – Показатели исходной защищенности ФГБУ «НПП «ГАММА»

|  |  |  |  |
| --- | --- | --- | --- |
| **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 объёму 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. | + |  |  |

При составлении перечня актуальных угроз безопасности ПДн каждой

степени исходной защищенности ставится в соответствие числовой

коэффициент, а именно:

0 – для высокой степени исходной защищенности;

5 – для средней степени исходной защищенности;

10 – для низкой степени исходной защищенности.

Под частотой (вероятностью) реализации угрозы понимается

определяемый экспертным путем показатель, характеризующий, насколько

вероятным является реализация конкретной угрозы безопасности ПДн для

данной ИСПДн в складывающихся условиях обстановки. Вводятся четыре

вербальных градации этого показателя:

**маловероятно** – отсутствуют объективные предпосылки для

осуществления угрозы (например, угроза хищения носителей информации

лицами, не имеющими легального доступа в помещение, где последние

хранятся);

**низкая вероятность** – объективные предпосылки для реализации угрозы

существуют, но принятые меры существенно затрудняют ее реализацию

(например, использованы соответствующие средства защиты информации);

**средняя вероятность** - объективные предпосылки для реализации

угрозы существуют, но принятые меры обеспечения безопасности ПДн

недостаточны;

**высокая вероятность** - объективные предпосылки для реализации

угрозы существуют, и меры по обеспечению безопасности ПДн не приняты.

При составлении перечня актуальных угроз безопасности ПДн каждой

градации вероятности возникновения угрозы ставится в соответствие

числовой коэффициент, а именно:

0 – для маловероятной угрозы;

2 – для низкой вероятности угрозы;

5 – для средней вероятности угрозы;

10 – для высокой вероятности угрозы.

С учетом изложенного коэффициент реализуемости угрозы Y будет

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

* если, то возможность реализации угрозы признается низкой;

если, то возможность реализации угрозы признается средней;

* если, то возможность реализации угрозы признается высокой;
* если, то возможность реализации угрозы признается очень высокой.

Далее оценивается опасность каждой угрозы. При оценке опасности на основе опроса экспертов (специалистов в области защиты информации) определяется вербальный показатель опасности для рассматриваемой

ИСПДн. Этот показатель имеет три значения:

**низкая опасность** – если реализация угрозы может привести к

незначительным негативным последствиям для субъектов персональных

данных;

**средняя опасность** – если реализация угрозы может привести к

негативным последствиям для субъектов персональных данных;

**высокая опасность** – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных

данных.

При составлении перечня актуальных угроз безопасности персональных данных каждой степени исходного уровня защищенности

ИСПДн ставится в соответствие числовой коэффициент Y₁, а именно:

0 – для высокой степени исходной защищенности;

5 – для средней степени исходной защищенности;

10 – для низкой степени исходной защищенности

Затем осуществляется выбор из общего (предварительного) перечня угроз безопасности тех, которые относятся к актуальным для данной ИСПДн, в соответствии с правилами, приведенными в таблице 6.

Таблица 6 – 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 университета: 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.

Таблица 7 – Показатели исходной защищенности ИСПДн

|  |  |  |  |
| --- | --- | --- | --- |
| **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 ИСПДн, развернутая в пределах одного здания | - | - | - |
| корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации; | - | + | - |
| **2. По наличию соединения с сетями общего пользования:** |  | + |  |
| ИСПДн, имеющая одноточечный выход в сеть общего пользования; | - | + | - |
| ИСПДн, имеющая многоточечный 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 объёму 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 | + | - | - |

По результатам, ИСПДн ФГБУ «НПП «ГАММА» соответствует среднему уровню защищенности.