|  |  |
| --- | --- |
|  | УТВЕРЖДАЮ  Руководитель органа  государственной власти  (организации) или иное  уполномоченное лицо  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_г. |

**Модель угроз безопасности информации защищённой автоматизированной информационной системы ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»**

г. Москва

2024 г.

СОДЕРЖАНИЕ

[1 ОБЩИЕ ПОЛОЖЕНИЯ 5](#_Toc156998878)

[1.1 Назначение и область действия документа 5](#_Toc156998879)

[1.2 Нормативные правовые акты, методические документы, национальные стандарты, используемые для оценки угроз безопасности информации и разработки модели угроз 6](#_Toc156998880)

[1.3 Наименование обладателя информации, заказчика, оператора систем и сетей 7](#_Toc156998881)

[1.4 Подразделения, должностные лица, ответственные за обеспечение защиты информации (безопасности) систем и сетей 7](#_Toc156998882)

[1.5 Наименование организации, привлекаемой для разработки модели угроз безопасности информации (при наличии) 7](#_Toc156998883)

[2 ОПИСАНИЕ СИСТЕМ И СЕТЕЙ И ИХ ХАРАКТЕРИСТИКА КАК ОБЪЕКТОВ ЗАЩИТЫ 8](#_Toc156998884)

[2.1. Наименование систем и сетей, для которых разработана модель угроз безопасности информации 8](#_Toc156998885)

[2.2. Класс защищенности, категория значимости систем и сетей, уровень защищенности персональных данных 8](#_Toc156998886)

[2.3. Нормативные правовые акты Российской Федерации, в соответствии с которыми создаются и (или) функционируют системы и сети 8](#_Toc156998887)

[2.4. Назначение, задачи (функции) систем и сетей, состав обрабатываемой информации и ее правовой режим 8](#_Toc156998888)

[2.5 Основные процессы обладателя информации, для обеспечения которых создаются (функционируют) системы и сеты 10](#_Toc156998889)

[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](#_Toc156998890)

[2.7 Описание функционирования систем и сетей на базе информативно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры: 11](#_Toc156998891)

[2.8 Описание модели предоставления вычислительных услуг, распределения ответственности за защиту информации между обладателями информации, оператором и поставщиком вычислительных услуг 12](#_Toc156998892)

[2.9 Описание условий использования информационно-телекоммуникационной инфраструктуры обработки данных или облачной инфраструктуры поставщика услуг (при наличии) 12](#_Toc156998893)

[3 ВОЗМОЖНЫЕ НЕГАТИВНЫЕ ПОСЛЕДСТВИЯ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. ВОЗМОЖНЫЕ ОБЪЕКТЫ ВОЗДЕЙСТВИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. ИСТОЧНИКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ 13](#_Toc156998894)

[4 СПОСОБЫ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ 17](#_Toc156998895)

[5 АКТУАЛЬНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИ 18](#_Toc156998896)

**ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ**

|  |  |  |
| --- | --- | --- |
| АИС | – | Автоматизированная информационная система |
| БД | – | База данных |
| ИСПДн | – | Информационная система персональных данных |
| ЛВС | – | Локальная вычислительная сеть |
| НИЦ | – | Национальный исследовательский центр |
| НСД | – | Несанкционированный доступ |
| ОС | – | Операционная система |
| ПДн | – | Персональные данные |
| ПИЯФ | – | Петербургский институт ядерной физики им. Б.П. Константинова |
| ПО | – | Программное обеспечение |
| ФГБУ | – | Федеральное государственное бюджетное учреждение |

# 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 АИС ФГБУ «ПИЯФ» НИЦ «Курчатовский институт».

Результаты определения актуальных угроз безопасности защищаемой информации предназначены для формирования обоснованных требований к составу и содержанию мер по обеспечению информационной безопасности АИС ФГБУ «ПИЯФ» НИЦ «Курчатовский институт».

Областью применения процесса определения угроз безопасности информации является совокупность информационных и программно-аппаратных элементов, а также информационных технологий, применяемых при обработке информации в АИС ФГБУ «ПИЯФ» НИЦ «Курчатовский институт».

Элементами АИС ФГБУ «ПИЯФ» НИЦ «Курчатовский институт» являются:

– информация заказчика, как совокупность информации и её носителей, используемых в АИС ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»;

– 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 ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»);

– средства защиты информации;

– подсистемы и сервисы, образуемые на основе технических и программных средств, средства защиты информации АИС ФГБУ «ПИЯФ» НИЦ «Курчатовский институт» (в том числе инфраструктурные подсистемы, инфраструктурные сервисы, подсистемы информационной безопасности).

# 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 Наименование обладателя информации, заказчика, оператора систем и сетей

Обладателем информации, заказчиком и оператором систем и сетей является ФГБУ «ПИЯФ» НИЦ «Курчатовский институт».

1.4 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 Института; работников, ответственных за администрирование сегментов информационной телекоммуникационной системы Института; работников, выполняющих следующие функции: администраторов информационных систем, администраторов локальной вычислительной сети, администраторов по обеспечению безопасности информации.

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 данных АСИ ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»;

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

– объект 3 – сервер, на котором хранятся БД ИСПДн, АСИ ФГБУ «ПИЯФ» НИЦ «Курчатовский институт».

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

Уровень защищенности ИСПДн АСИ ФГБУ «ПИЯФ» НИЦ «Курчатовский институт» – первый (т.к. в ИСПДн обрабатываются иные категории ПДн и на объекте отсутствуют сертифицированное прикладное ПО по требованиям безопасности).

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

АСИ ФГБУ «ПИЯФ» НИЦ «Курчатовский институт» разработана в соответствии с положениями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее в тексте – Закон № 152-ФЗ), 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 учащихся с целью обеспечения безопасности от несанкционированного доступа на объект посторонних людей, порчи имущества, наблюдение за поведением учащихся, а также хранение всей информации на сервере.

Персональные данные студентов в АСИ ФГБУ «ПИЯФ» НИЦ «Курчатовский институт» обрабатываются с целью:

– организации учебного процесса;

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

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

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

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

Персональные данные учащихся включают в себя:

– фамилию, имя, отчество студента;

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

– дату рождения студента;

– адрес проживания студента;

– фамилию, имя, отчество родителей.

Персональные данные сотрудников ФГБУ «ПИЯФ» НИЦ «Курчатовский институт» 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 «ПИЯФ» НИЦ «Курчатовский институт» 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 студентов, 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 (главный администратор, директор института) | 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 (бухгалтерия) | 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 (преподаватели) | Обладают информацией о системном и прикладном программном обеспечении ИСПДн | Уточнение, использование |
| Пользователи, являющиеся внешними по отношению к ИСПДн (студенты) | Отсутствует | Отсутствует |
| Обслуживающий персонал (уборщицы, повара и т.д.) | 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

Таблица 2 – Определение модели предоставления вычислительных услуг

|  |  |  |
| --- | --- | --- |
| **Услуга** | **Ответственность поставщика Mail.ru Group** | **Ответственность оператора** |
| Предоставление сервера для хранения ИСПДн | Приложения, среда выполнения, связующее ПО, платформа виртуализации ОС аппаратная платформа, система хранения данных, сетевая инфраструктура | Данные |

# 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

Таблица 3 – Возможные цели реализации угроз безопасности информации нарушителями

|  |  |  |  |
| --- | --- | --- | --- |
| **№ вида** | **Виды нарушителя** | **Категория нарушителя** | **Возможные цели реализации угроз безопасности информации** |
| 1 | Террористические, экстремистские группировки | Внешний | Совершение террористических актов, угроза жизни граждан. Нанесение ущерба отдельным сферам деятельности или секторам экономики государства. Дестабилизация общества. Дестабилизация деятельности органов государственной власти, организаций. |
| 2 | Отдельные физические лица (хакеры) | Внешний | Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса). |
| 3 | Разработчики программных, программно-аппаратных средств | Внутренний | Внедрение дополнительных функциональных возможностей в программные или программно-аппаратные средства на этапе разработки. Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. |
| 4 | Лица, обеспечивающие постановку программных, программно-аппаратных средств, обеспечивающих систем | Внешний | Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ. |
| 5 | 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. |

Таблица 4 – Соответствие возможных целей реализации угроз безопасности информации с негативными последствиями

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№** | **Вид нарушителя** | **Цели реализации угроз безопасности информации** | **Вид риска (ущерба)** | | |
| Нанесение ущерба физическому лицу | Нанесение ущерба юридическому лицу, индивидуальному предпринимателю | Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности |
| 1 | Отдельные физические лица (хакеры) | Получение финансовой или иной материальной выгоды | НП1, НП2 | НП2, НП3, НП6 | - |
| 2 | Авторизованные пользователи систем и сетей | Любопытство или желание самореализации. Непреднамеренные, неосторожные или неквалифицированные действия | НП1, НП2 | - | - |
| 3 | Разработчики программных, программно-аппаратных средств | Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. | НП1, НП2 | НП2, НП3, НП4, НП5, НП6 | - |
| 4 | Лица, обеспечивающие постановку программных, программно-аппаратных средств, обеспечивающих систем | Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ. | НП1, НП2 | НП2, НП3, НП4, НП5, НП6 | - |
| 5 | Террористические, экстремистские группировки | Совершение террористических актов, угроза жизни граждан. Нанесение ущерба отдельным сферам деятельности или секторам экономики государства. | - | - | Дестабилизация деятельности органов государственной власти, организаций |

Таблица 5 – Описание групп пользователей

|  |  |  |
| --- | --- | --- |
| **Негативные последствия** | **Объекты воздействия** | **Виды воздействия** |
| Потеря (хищение) данных | Серверы и хранилища данных | Несанкционированная подмена данных, содержащихся на серверах |
| АРМы бухгалтерии | Подмена данных, содержащих реквизиты платежных поручений и другой платежной информации на АРМ главного бухгалтера |
| АРМы финансового департамента | Подмена данных, переделанная информации в платежных распоряжениях и отправка недостоверных распоряжений от имени финансового директора |
| Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса | АРМы отдела Информационной безопасности | Модификация информации и отправка электронных писем с недостоверной информацией от имени руководителя организации |
| АРМ главного инженера/администратора | Несанкционированная отправка команд, приводящая к несрабатыванию средств аварийной защиты и (или) к изменению логики ПЛК |
| Недоступность данных | Серверы и хранилища данных | Несанкционированная отправка команд, приводящая к несрабатыванию средств аварийной защиты |
| Программное обеспечение | Несанкционированная отправка команд, приводящая к остановке бизнес процессов |
| Сетевая инфраструктура | Несанкционированная модификация (изменение) логики работы или установок коммутационного контроллера, которая приводит к остановке бизнес-процессов |
| Утечка персональных данных | Серверы и хранилища данных | Нарушение безопасности может привести к утечке персональных данных, что может вызвать ущерб репутации предприятия и привести к юридическим последствиям. |

# 4 СПОСОБЫ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Таблица 6 – Способы реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности

|  |  |  |  |
| --- | --- | --- | --- |
| **Вид нарушителя** | **Категория нарушителя** | **Объекты воздействия** | **Способы реализации** |
| Отдельные физические лица (хакеры) | Внешний | Телекоммуникационное оборудование | СР1, СР2, СР7, СР10 |
| Информация (данные), содержащаяся в системах и сетях | СР8 |
| Разработчики программных, программно-аппаратных средств | Внутренний | Программно-аппаратные средства обработки и хранения информации | СР1, СР2, СР3, СР6, СР7, СР9 |
| Машинные носители информации, содержащие как защищаемую информацию, так и аутентификационную информацию | СР6, СР7, СР9 |
| Авторизованные пользователи систем и сетей | Внутренний | Программно-аппаратные средства обработки и хранения информации | СР1, СР2, СР3, СР6, СР7, СР9 |
| Машинные носители информации, содержащие как защищаемую информацию, так и аутентификационную информацию | СР8, СР9, СР10 |
| Лица, обеспечивающие постановку программных, программно-аппаратных средств, обеспечивающих систем | Внешний | Программно-аппаратные средства обработки и хранения информации | СР1, СР2, СР3, СР6, СР7, СР9 |
| Машинные носители информации, содержащие как защищаемую информацию, так и аутентификационную информацию | СР6, СР7, СР9 |

# 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 ФГБУ «ПИЯФ» НИЦ «Курчатовский институт» приведены в таблице 7.

Таблица 7 – Показатели исходной защищенности ИСПДн ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»

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

Значению уровня защищенности «Высокий» соответствуют 2 характеристики, значению уровня «Средний» - 4 характеристики, значению уровня «Низкий» - 1 характеристика. Таким образом, числовой коэффициент исходной защищенности ИСПДн ФГБУ «ПИЯФ» НИЦ «Курчатовский институт» 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 8.

Таблица 8 – 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.

Для данной типовой модели возможна реализация следующих угроз безопасности ПДн (табл. 9).

Таблица 9 – 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 |