УТВЕРЖДАЮ

Директор ГБОУ СО «Верхнесинячихинская
школа-интернат»

\_\_\_\_\_\_\_\_\_\_\_\_\_ О.А. Бурухина

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_2020 г.

м.п.

**Частная модель угроз безопасности персональных данных, обрабатываемых в информационной системе персональных данных**

**«Кадры»**

пгт. Верхняя Синячиха

2020 г.

**Содержание**

[Используемые сокращения и определения 3](#_Toc26741871)

[1 Общие положения 4](#_Toc26741872)

[2 Описание информационной системы персональных данных 6](#_Toc26741873)

[2.1 Назначение и цели функционирования ИСПДн 6](#_Toc26741874)

[2.2 Общие сведения об ИСПДн 6](#_Toc26741875)

[2.2.1 Место расположения ИСПДн 6](#_Toc26741876)

[2.2.2 Состав ИСПДн 6](#_Toc26741877)

[2.2.3 Сведения об обрабатываемой в ИСПДн информации 6](#_Toc26741878)

[2.2.4 Описание обработки ПДн в ИСПДн 6](#_Toc26741879)

[2.2.5 Взаимодействие с сетями общего пользования 7](#_Toc26741880)

[2.2.6 Заданные свойства безопасности 7](#_Toc26741881)

[2.3 Определение уровня защищенности ИСПДн 7](#_Toc26741882)

[2.4 Структурно-функциональные характеристики ИСПДн 8](#_Toc26741883)

[2.4.1 Программное обеспечение системы 8](#_Toc26741884)

[2.4.2 Аппаратное обеспечение 9](#_Toc26741885)

[3 Модель вероятного нарушителя информационной безопасности 10](#_Toc26741886)

[3.1 Описание возможных нарушителей 10](#_Toc26741887)

[3.1.1 Внешний нарушитель 10](#_Toc26741888)

[3.1.2 Внутренний нарушитель 10](#_Toc26741889)

[3.2 Предположения об имеющихся у нарушителя информации об объектах атак 11](#_Toc26741890)

[3.3 Предположения об имеющихся у нарушителя средствах атак 12](#_Toc26741891)

[3.4 Описание каналов реализации атак 12](#_Toc26741892)

[4 Определение уровня исходной защищенности информационной системы 13](#_Toc26741893)

[4.1 Определение уровня исходной защищенности ИСПДн 13](#_Toc26741894)

[5 Методика определения актуальных угроз информационной системы 15](#_Toc26741895)

[5.1 Частота (вероятность) реализации угрозы 15](#_Toc26741896)

[5.2 Реализация угрозы 15](#_Toc26741897)

[5.3 Опасность угроз 15](#_Toc26741898)

[5.4 Выбор актуальных угроз 16](#_Toc26741899)

[6 Перечень основных угроз безопасности информации в ИСПДн 17](#_Toc26741900)

[7 Перечень угроз информации 19](#_Toc26741901)

### Используемые сокращения и определения

Таблица 1- Сокращения

|  |  |
| --- | --- |
| АРМ | Автоматизированное рабочее место |
| БД | Базы данных |
| ВТСС | Вспомогательные технические средства и системы |
| ИС  | Информационная система |
| ИСПДн | Информационные системы персональных данных |
| НСД | Несанкционированный доступ |
| ОС | Операционная система |
| ОТСС | Основные технические средства и системы |
| ПАК | Программно-аппаратный комплекс |
| ПДн  | Персональные данные |
| ПО | Программное обеспечение |
| СЗИ  | Система защиты информации |
| СУБД | Система управления базами данных |
| УБПДн  | Угрозы безопасности персональных данных |
| ФСТЭК России | Федеральная служба по техническому и экспортному контролю |
| ЦОД | Центр обработки данных |

# Общие положения

Разработка Частной модели угроз безопасности персональных данных, обрабатываемых в информационной системе персональных данных «Кадры» (далее – ИСПДн), проведена в соответствии со следующими действующими нормативно-методическими документами в области защиты информации:

* Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
* Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных».
* Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
* Приказ Федеральной службы по техническому и экспортному контролю России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
* Методика определения актуальных угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена 14 февраля 2008г. заместителем директора ФСТЭК России).
* Базовая модель угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена 15 февраля 2008г. заместителем директора ФСТЭК России).

Под угрозами безопасности информации при её обработке в информационных системах персональных данных (далее – угрозами) понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на нее.

Угрозы безопасности могут быть реализованы за счет утечки информации по техническим каналам (технические каналы утечки информации, обрабатываемой ЭВМ; технические каналы перехвата информации при ее передаче по каналам связи; технические каналы утечки акустической (речевой) информации), либо за счет несанкционированного доступа к ИСПДн или базам данных с использованием штатного или специально разработанного программного обеспечения.

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

Частная модель угроз разработана с учетом назначения, условий и особенностей функционирования ИСПДн.

Частная модель угроз используется при разработке системы защиты информации, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты, предусмотренных для соответствующего необходимого класса ИСПДн.

Настоящая модель угроз может быть пересмотрена:

* по решению оператора при изменениях масштаба, расположения, конфигурации, режима функционирования информационной системы или значимости обрабатываемой в ней информации т.п.;
* по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности информации при её обработке в ИСПДн.

# Описание информационной системы персональных данных

## Назначение и цели функционирования ИСПДн

ГБОУ СО «Верхнесинячихинская школа-интернат» (далее – Оператор) является государственным бюджетным общеобразовательным учреждением Свердловской области «Верхнесинячихинская школа-интернат, реализующая адаптированные основные общеобразовательные программы».

Информационная система персональных данных «Кадры» предназначена для информационно-технологического сопровождения кадрового делопроизводства в ГБОУ СО «Верхнесинячихинская школа-интернат».

## Общие сведения об ИСПДн

* + 1. Место расположения ИСПДн

Вычислительные мощности ИСПДн размещены на территории Оператора.

* + 1. Состав ИСПДн

Основными элементами ИСПДн являются:

* информация, содержащаяся в информационной системе;
* технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической, видео- и речевой информации);
* общесистемное, прикладное, специальное программное обеспечение;
* информационные технологии;
* средства защиты информации;
* средства криптографической защиты информации.
	+ 1. Сведения об обрабатываемой в ИСПДн информации

В информационной системе обрабатываются сведения следующих категорий:

* сведения ограниченного доступа, в том числе персональные данные.
	+ 1. Описание обработки ПДн в ИСПДн

В ИСПДн обрабатываются ПДн следующих категорий субъектов ПДн:

* Граждане РФ.
* Сотрудники Оператора.
* Родственники сотрудников Оператора.

В ИСПДн обрабатываются ПДн сотрудников Оператора, относимые к категориям ПДн «иные».

В ИСПДн обрабатываются ПДн граждан РФ, не являющиеся сотрудников Оператора, относимые к категориям ПДн «иные».

Объем ПДн, обрабатываемых в ИСПДн, менее 100 000 субъектов.

* + 1. Взаимодействие с сетями общего пользования

По наличию подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена ИСПДн относится к системам, имеющим подключение.

* + 1. Заданные свойства безопасности

Устанавливаются следующие свойства безопасности для защищаемой информации, приведенные в таблице ниже (см. Таблица 2 - Свойства безопасности).

Таблица 2 - Свойства безопасности

| **№ п/п** | **Характеристика безопасности** | **Наличие характеристики безопасности** |
| --- | --- | --- |
|  | Конфиденциальность | Да |
|  | Целостность | Да |
|  | Доступность | Да |

## Определение уровня защищенности ИСПДн

В качестве системного ПО используется стабильная лицензионная версия операционной системы Windows, получающая регулярные обновления, а также являющаяся программным обеспечением с закрытым исходным кодом.

В качестве прикладного ПО используются стабильные лицензионные версии программных продуктов, получающие регулярные обновления и имеющие закрытый исходный код.

Учитывая вышеприведённые факты, можно говорить о неактуальности угроз, связанных с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в ИСПДн.

Учитывая вышесказанное, можно говорить о неактуальности угроз, связанных с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в ИСПДн.

Таким образом, для ИСПДн актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе (угрозы 3-его типа).

Персональные данные, обрабатываемые в ИСПДн, могут быть отнесены к категориям «иные».

Субъектами персональных данных, обрабатываемых в ИСПДн, являются граждане РФ, сотрудники Оператора, родственники сотрудников.

Количество субъектов, чьи персональные данные обрабатываются в ИСПДн, менее 100 000.

Принцип классификации в соответствие с постановлением правительства №1119 от 1 ноября 2012 года «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» отображен в Таблице 3.

Таблица 3 – Определение уровня защищённости ПДн

|  |  |  |  |
| --- | --- | --- | --- |
| Тип категории персональных данных | Категория субъектов | Количество субъектов | Тип актуальных угроз |
| 1 тип | 2 тип | 3тип |
| Специальные | Не сотрудники | Более 100 000 | УЗ 1 | УЗ 1 | УЗ 2 |
| Менее 100 000 | УЗ 1 | УЗ 2 | УЗ 3 |
| Сотрудники | Более 100 000 | УЗ 1 | УЗ 2 | УЗ 3 |
| Менее 100 000 | УЗ 1 | УЗ 2 | УЗ 3 |
| Биометрические | Не сотрудники | Более 100 000 | УЗ 1 | УЗ 2 | УЗ 3 |
| Менее 100 000 | УЗ 1 | УЗ 2 | УЗ 3 |
| Сотрудники | Более 100 000 | УЗ 1 | УЗ 2 | УЗ 3 |
| Менее 100 000 | УЗ 1 | УЗ 2 | УЗ 3 |
| Иные | Не сотрудники | Более 100 000 | УЗ 1 | УЗ 2 | УЗ 3 |
| Менее 100 000 | УЗ 1 | УЗ 3 | УЗ 4 |
| Сотрудники | Более 100 000 | УЗ 1 | УЗ 3 | УЗ 4 |
| Менее 100 000 | УЗ 1 | УЗ 3 | УЗ 4 |
| Общедоступные | Не сотрудники | Более 100 000 | УЗ 2 | УЗ 3 | УЗ 4 |
| Менее 100 000 | УЗ 2 | УЗ 3 | УЗ 4 |
| Сотрудники | Более 100 000 | УЗ 2 | УЗ 3 | УЗ 4 |
| Менее 100 000 | УЗ 2 | УЗ 3 | УЗ 4 |

 В соответствие с Таблицей 3 ИСПДн может быть присвоен четвертый уровень защищенности.

## Структурно-функциональные характеристики ИСПДн

### Программное обеспечение системы

В качестве программного обеспечения используется следующий состав программных средств:

АРМ Запольских:

* Microsoft Windows XP.
* Microsoft Office Professional 2007.
* АС «Интернет-банк» 2.9.
* Контур-Бухгалтерия Бюджет 7.0.5.
* Контур-Зарплата 4.5.
* Контур-Персонал 1.21.06.
* Google Chrome.
* Перечень льготных профессий 3.6.
* Контур-Экстерн.
* ПФ-Отчет + 2-НДФЛ.

### Аппаратное обеспечение

Аппаратное обеспечение представлено автоматизированным рабочим местом в составе системного блока, монитора, манипулятора «мышь», клавиатуры и принтера, расположенными по адресу: пгт. Верхняя Синячиха, ул. Черепановская, д. 13.

Доступ в локальную сеть и сеть Интернет осуществляется через коммутаторы D-Link DGS-1100-26/ME и TP-Link TD-W8951ND. .

# Модель вероятного нарушителя информационной безопасности

Описание возможных нарушителей

По признаку принадлежности к ИСПДн все нарушители делятся на две группы:

* Внешние нарушители – физические лица, не имеющие права пребывания на территории, в пределах которой размещена ИСПДн.
* Внутренние нарушители – физические лица, имеющие право пребывания на территории, в пределах которой размещена ИСПДн.

### Внешний нарушитель

В качестве внешнего нарушителя информационной безопасности, рассматривается нарушитель, который не имеет непосредственного доступа к техническим средствам и ресурсам системы.

ИСПДн имеет подключение к сетям связи общего пользования и (или) сетям международного информационного обмена. Внешние нарушители, имеющие потенциальную возможность реализации атаки по данному каналу, относятся к вероятным нарушителям.

Предполагается, что внешний нарушитель не будет воздействовать на защищаемую информацию по техническим каналам утечки, так как объем и значимость информации, хранимой и обрабатываемой в ИСПДн, являются недостаточными для проведения крайне дорогостоящих и трудоемких атака, направленных на добывание информации по техническим каналам утечки.

### Внутренний нарушитель

Возможности внутреннего нарушителя зависят от действующих ограничительных факторов, из которых в основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовке кадров, допуску физических лиц к техническим средствам и ресурсам системы, и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированных действий.

Исходя из особенностей функционирования ИСПДн, допущенные к ней физические лица, имеют разные полномочия на доступ к ресурсам системы. К внутренним нарушителям могут относиться:

* Персонал сторонних организаций, уполномоченный администрировать инфраструктуру и ПО ИСПДн, но не имеющий доступ к персональным данным (категория 1).
* Зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн (категория 2).
* Персонал Оператора, обладающий административными правами для доступа к ПО, инфраструктуре и средствам защиты информации ИСПДн (категория 5).
* Разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на ИСПДн (категория 8).

Лица, относящиеся к категориям 1, 2 и 5 относятся к вероятным нарушителям. Лица, относящиеся к категории 8 не рассматриваются в качестве вероятных нарушителей поскольку не будут рисковать имиджем компании ради незначительной экономической выгоды.

На лиц, относящихся к категории 1 возложены задачи по администрированию программно-аппаратных средств и баз данных ИСПДн. Администраторы потенциально могут реализовать угрозы ИБ, используя возможности по непосредственному доступ к защищаемой информации, обрабатываемой и хранимой в ИСПДн, а также к техническим и программным средствам ИСПДн, включая средства защиты, используемые в ИСПДн, в соответствии с установленными для них административными правами. Лица, относящиеся к данным категориям, хорошо знакомы с основными принципами, алгоритмами, протоколами, реализуемыми в ИСПДн, а также с применяемыми мерами в области защиты информации.

Предполагается, что они могут использовать стандартное оборудование для идентификации уязвимостей, либо для реализации угроз информационной безопасности. Данное оборудование может быть, как частью штатных средств, так и может относиться к легко получаемому оборудованию. Так же возможен факт обладания данными лицами специализированного оборудования или программных средств.

Лица, относящиеся к категории 1, являются сотрудниками сторонних организаций. Между Оператором и данными организациями заключены соглашения о конфиденциальности, обязующее весь персонал, имеющий доступ к инфраструктуре ИСПДн, ПО и данным, циркулирующим в ней, обеспечивать необходимый уровень защищённости.

К лицам категории 2 и 5 применяется комплекс особых организационных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения ими своих должностных обязанностей.

Лица, относящиеся к категории 2 и 5 выбираются из доверенных лиц и поэтому они исключаются из числа вероятных нарушителей.

Предполагается, что сговор внутренних нарушителей маловероятен в силу принятых организационных и контролирующих мер.

## Предположения об имеющихся у нарушителя информации об объектах атак

*В качестве основных уровней знаний нарушителей об ИСПДн можно выделить следующие:*

* Информация о назначении и общих характеристиках ИСПДн.
* Информация, полученная из эксплуатационной документации на ИСПДн.
* Информация, полученная из проектной документации на ИСПДн.

*Нарушитель может иметь:*

* Информацию об организации работы, архитектуре, используемых технических и программных решениях.
* Сведения об информационных ресурсах: порядок и правила создания, хранения, передачи информации. Структура и свойства информации.
* Данные об уязвимостях и каналах реализации угроз в ИСПДн.
* Сведения о реализованных мерах по обеспечению информационной безопасности данных, циркулирующих в ИСПДн.
* Исходные коды программного обеспечения, используемого в ИСПДн.

Предполагается, что лица, отнесенные к категории 1 и 5, обладают информацией, содержащейся в эксплуатационной документации на ИСПДн.

Предполагается, что лица, отнесенные к категории 2, обладают только информацией о функционале системы.

Предполагается, что лица категории 8 имеют права на санкционированное нахождение в помещениях, в которых располагаются вычислительные ресурсы ИСПДн. Однако, лица данных категорий не имеют парольной информации на доступ к персональным данным в ИСПДн.

Таким образом, наиболее информированными об ИСПДн являются лица категории 1 и 5.

Предположения об имеющихся у нарушителя средствах атак

Предполагается, что нарушитель может иметь:

* Аппаратные компоненты ИСПДн.
* Доступные в свободной продаже технические и программные средства.
* Специально разработанные технические и программные средства.

Предполагается, что нарушитель имеет все необходимые для проведения атак по доступным ему каналам атак средства, возможности которых не превосходят возможности аналогичных средств атак на информацию, содержащую сведения, составляющие государственную тайну.

Так же предполагается, что в силу отсутствия целесообразности приобретения дорогостоящего оборудования, для перехвата информации, циркулирующей в ИСПДн, нарушитель не обладает:

* Средствами перехвата по техническим каналам утечки.
* Средствами воздействия через сигнальные цепи.
* Средствами воздействия на источники и через цепи питания.
* Средствами воздействия через цепи заземления.
* Средствами активного воздействия на ОТСС ИСПДн.

Предполагается, что наиболее совершенными средствами реализации угроз обладают лица категорий 1, 2 и 5.

Описание каналов реализации атак

Каналами реализации угроз ИБ ИСПДн являются:

* каналы непосредственного доступа к объекту атаки (акустический, визуальный, физический);
* машинные носители информации;
* носители информации, выведенные из употребления;
* технические каналы утечки;
* сигнальные цепи;
* цепи электропитания;
* цепи заземления;
* канал утечки за счет электронных устройств негласного получения информации;
* информационные и управляющие интерфейсы СВТ.

# Определение уровня исходной защищенности информационной системы

Определение уровня исходной защищенности ИСПДн

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн, приведенных в таблице ниже (см. Уровень исходной защищенности ИСПДн).

Таблица 4 – Уровень исходной защищенности ИСПДн

| **Технические и эксплуатационные характеристики ИСПДн** | **Уровень защищенности** |
| --- | --- |
| **Высокий** | **Средний** | **Низкий** |
| 1. По территориальному размещению:- локальная ИСПДн, развернутая в пределаходного здания. | + | - | - |
| 2. По наличию соединения с сетями общего пользования:- ИСПДн, имеющая одноточечный выход в сеть общего пользования. | - | + | - |
| 3. По встроенным (легальным) операциям с записями баз персональных данных:- запись, удаление, сортировка. | - | + | - |
| 4. По разграничению доступа к персональным данным: |  |  |  |
| - ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн. | - | + | - |
| 5. По наличию соединений с другими базами данных иных ИСПДн: |  |  |  |
| - ИСПДн, в которой используется одна база данных, принадлежащая организации – владельцу данной ИСПДн. | + | - | - |
| 6. По уровню обобщения (обезличивания) ПДн:- ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн). | - | - | + |
| 7. По объему данных, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки: | - | + | - |
| - ИСПДн, предоставляющая часть ПДн. |  |  |  |
| **Процентное соотношение** | **28,57%** | **57,14%** | **14,29%** |

В соответствие с полученными данными устанавливается средний показатель исходной защищенности, так не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний», а остальные – низкому уровню защищенности. При составлении перечня актуальных угроз ИСПДн среднему уровню исходной защищенности ставится в соответствие числовой коэффициент Y1 равный 5.

# Методика определения актуальных угроз информационной системы

Для оценки актуальности угрозы применяются два показателя: уровень исходной защищенности ИСПДн и частота (вероятность) реализации рассматриваемой угрозы.

Частота (вероятность) реализации угрозы

Под частотой (вероятностью) реализации угрозы понимается определенный экспертным путем показателя, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности для ИСПДн в складывающихся условиях обстановки.

Используются четыре значения этого показателя:

* маловероятно – отсутствуют объективные предпосылки для осуществления угрозы;
* низкая вероятность – объективные предпосылки для реализации угрозы существуют, но применяемые меры существенно затрудняют ее реализацию;
* средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности недостаточны;
* высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры обеспечения безопасности не приняты.

При составлении перечня актуальных угроз каждому значению показателя ставится в соответствие числовой коэффициент Y2, а именно:

* 0 – для маловероятной угрозы;
* 2 – для низкой вероятности угрозы;
* 5 – для средней вероятности угрозы;
* 10 – для высокой вероятности угрозы.

Реализация угрозы

Коэффициент реализуемости угрозы Y определяется соотношением:

Y = (Y1 + Y2) / 20.

По значению коэффициента реализуемости угрозы Y формируется интерпретация реализуемости угрозы:

* 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.

Опасность угроз

При оценке опасности угрозы на основе опроса экспертов (специалистов в области защиты информации) определяется показатель опасности угрозы. Этот показатель имеет три значения:

* низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъекта персональных данных;
* средняя опасность – если реализация угрозы может привести к негативным последствиям для субъекта персональных данных;
* высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъекта персональных данных.

Выбор актуальных угроз

Выбор из общего (предварительного) перечня актуальных угроз для ИСПДн осуществляется в соответствии с правилами, приведенными в таблице ниже (см. Таблица 5 – Выбор актуальных угроз).

Таблица 5 – Выбор актуальных угроз

|  |  |
| --- | --- |
| **Возможность реализации угрозы (Y)** | **Показатель опасности угрозы** |
| **Низкая** | **Средняя** | **Высокая** |
| Низкая | неактуальная | неактуальная | актуальная |
| Средняя | неактуальная | актуальная | актуальная |
| Высокая | актуальная | актуальная | актуальная |
| Очень высокая | актуальная | актуальная | актуальная |

# Перечень основных угроз безопасности информации в ИСПДн

Угрозы, в соответствие с методическими документам ФСТЭК России, могут классифицироваться в соответствии со следующими признаками:

*По видам возможных источников угроз:*

* угрозы, связанные с действиями лиц, имеющих доступ к ИС (внутренний нарушитель);
* угрозы, связанные с действиями лиц, не имеющих доступ к ИС (внешний нарушитель);
* внедрение аппаратных закладок и вредоносных программ.

*По структуре ИС, на которые направлена реализация угроз:*

* угрозы в ИС на базе АРМ;
* угрозы в ИС на базе локальных информационных систем;
* угрозы в ИС на базе распределенных информационных систем.

*По виду несанкционированных действий, осуществляемых с информацией:*

* угрозы, приводящие к нарушению конфиденциальности информацией (нет непосредственного воздействия на информацию);
* угрозы, приводящие к несанкционированному воздействию на содержание информации (изменение или уничтожение информации);
* угрозы, приводящие к несанкционированному воздействию на программные или программно-аппаратные элементы ИС (блокирование информации).

*По способам реализации угроз:*

* угрозы, реализуемые в ИС при их подключении к сетям связи общего пользования;
* угрозы, реализуемые в ИС при их подключении к сетям международного информационного обмена;
* угрозы, реализуемые в ИС, не имеющих подключений к сетям связи общего пользования и сетям международного информационного обмена.

*По виду каналов, с использованием которых реализуется угроза:*

* угрозы, реализуемые через технические каналы утечки;
* угрозы, реализуемые за счет НСД к информации;
* угрозы специальных воздействий на ИС.

*По используемой уязвимости имеются угрозы следующих классов:*

* угрозы, реализуемые с использованием уязвимости системного ПО;
* угрозы, реализуемые с использованием уязвимости прикладного ПО;
* угрозы, возникающие в результате использования уязвимости, вызванной наличием в ИС аппаратной закладки;
* угрозы, реализуемые с использованием уязвимостей протоколов сетевого взаимодействия и каналов передачи данных;
* угрозы, возникающие в результате использования уязвимости, вызванной недостатками организации ТЗИ от НСД;
* угрозы, реализуемые с использованием уязвимостей, обусловливающих наличие технических каналов утечки информации;
* угрозы, реализуемые с использованием уязвимостей СЗИ.

# Перечень угроз информации

Таблица 6 - **Оценочные показатели угроз**

| **Угроза** | **Исходная защищенность****(Y1)** | **Частота реализации угрозы (Y2)** | **Коэффициент реализуемости угрозы Y.** | **Возможность реализации угрозы** | **Показатель опасности угрозы** | **Актуальность угрозы** |
| --- | --- | --- | --- | --- | --- | --- |
| Угроза, реализуемая за счет утечки акустической (речевой) информации | 5 | Маловероятная(Y2=0) | 0.25 | Низкая | Низкая | Угроза не актуальна |
| Угроза, реализуемая за счет утечки видовой информации | 5 | Маловероятная(Y2=0) | 0.25 | Низкая | Низкая | Угроза не актуальна |
| Угроза, реализуемая за счет утечки информации по каналам ПЭМИН | 5 | Маловероятная(Y2=0) | 0.25 | Низкая | Низкая | Угроза не актуальна |
| Кража сервера, АРМ, носителей информации | 5 | Низкая(Y2=2) | 0.35 | Средняя | Средняя | Угроза актуальна |
| Вывод из строя узлов и каналов связи | 5 | Низкая(Y2=2) | 0.35 | Средняя | Низкая | Угроза не актуальна |
| Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов | 5 | Маловероятная(Y2=0) | 0.25 | Низкая | Низкая | Угроза не актуальна |
| Несанкционированное копирование | 5 | Низкая(Y2=2) | 0.35 | Средняя | Низкая | Угроза не актуальна |
| Несанкционированная передача по каналам связи | 5 | Маловероятно(Y2=0) | 0.25 | Низкая | Низкая | Угроза не актуальна |
| Несанкционированное отключение средств защиты | 5 | Низкая(Y2=2) | 0.35 | Средняя | Средняя | Угроза актуальна |
| Угрозы, реализуемые за счет уязвимостей в микропрограммах и средствах операционных систем | 5 | Маловероятно(Y2=0) | 0.25 | Низкая | Низкая | Угроза не актуальна |
| Угрозы, реализуемые за счет фрагментов кода в микропрограммах и средствах операционных систем | 5 | Маловероятно(Y2=0) | 0.25 | Низкая | Средняя | Угроза не актуальна |
| Угрозы, реализуемые за счет отсутствия необходимых средств защиты | 5 | Средняя(Y2=5) | 0.5 | Средняя | Средняя | Угроза актуальна |
| Угрозы, реализуемые за счет ошибок в системном программном обеспечении | 5 | Маловероятно(Y2=0) | 0.25 | Низкая | Средняя | Угроза не актуальна |
| Угрозы, реализуемые за счет уязвимостей в протоколах сетевого взаимодействия | 5 | Средняя(Y2=5) | 0.5 | Средняя | Средняя | Угроза актуальна |
| Угрозы, реализуемые за счет несовместимости разных прикладных программа | 5 | Маловероятно(Y2=0) | 0.25 | Низкая | Средняя | Угроза не актуальна |
| Угрозы, реализуемые за счет изменения параметров прикладных программ | 5 | Низкая(Y2=2) | 0.35 | Средняя | Средняя | Угроза актуальна |
| Угрозы, реализуемые за счет фрагментов кода прикладных программ | 5 | Маловероятно(Y2=0) | 0.25 | Низкая | Средняя | Угроза не актуальна |
| Угрозы, реализуемые за счет ошибок в прикладных программах | 5 | Маловероятно(Y2=0) | 0.25 | Низкая | Средняя | Угроза не актуальна |
| Угрозы, реализуемые в ходе загрузки ОС | 5 | Маловероятно(Y2=0) | 0.25 | Низкая | Средняя | Угроза не актуальна |
| Угрозы, реализуемые после загрузки операционной среды | 5 | Низкая(Y2=2) | 0.35 | Средняя | Средняя | Угроза актуальна |
| Угрозы анализа сетевого трафика | 5 | Низкая(Y2=2) | 0.35 | Средняя | Средняя | Угроза актуальна |
| Угрозы сканирования сети | 5 | Средняя(Y2=5) | 0.5 | Средняя | Средняя | Угроза актуальна |
| Угрозы выявления пароля | 5 | Низкая(Y2=2) | 0.35 | Средняя | Средняя | Угроза актуальна |
| Угроза подмены доверенного объекта сети, и передача по каналам связи сообщений от его имени с присвоением его прав доступа | 5 | Маловероятная(Y2=0) | 0.25 | Низкая | Низкая | Угроза не актуальна |
| Угроза навязывания ложного маршрута сети | 5 | Низкая(Y2=2) | 0.35 | Средняя | Средняя | Угроза актуальна |
| Угроза внедрения ложного объекта сети | 5 | Маловероятная(Y2=0) | 0.25 | Низкая | Низкая | Угроза не актуальна |
| Скрытый отказ в обслуживании | 5 | Маловероятная(Y2=0) | 0.25 | Низкая | Низкая | Угроза не актуальна |
| Явный отказ в обслуживании, вызванный исчерпанием ресурсов ИС | 5 | Маловероятная(Y2=0) | 0.25 | Низкая | Низкая | Угроза не актуальна |
| Явный отказ в обслуживании, вызванный нарушением логической связности | 5 | Маловероятная(Y2=0) | 0.25 | Низкая | Низкая | Угроза не актуальна |
| Явный отказ в обслуживании, вызванный использованием ошибок в ПО | 5 | Маловероятная(Y2=0) | 0.25 | Низкая | Низкая | Угроза не актуальна |
| Удаленный запуск приложений, содержащих несанкционированный исполняемый код | 5 | Низкая(Y2=2) | 0.35 | Средняя | Средняя | Угроза актуальна |
| Удаленный запуск приложений путем переполнения буфера приложений-серверов | 5 | Маловероятная(Y2=0) | 0.25 | Низкая | Низкая | Угроза не актуальна |
| Удаленный запуск приложения путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками либо используемыми штатными средствами | 5 | Маловероятная(Y2=0) | 0.25 | Низкая | Низкая | Угроза не актуальна |
| Внедрение загрузочных вирусов | 5 | Низкая(Y2=2) | 0.35 | Средняя | Средняя | Угроза актуальна |
| Внедрение замещающих вирусов | 5 | Низкая(Y2=2) | 0.35 | Средняя | Средняя | Угроза актуальна |
| Внедрение паразитических вирусов | 5 | Низкая(Y2=2) | 0.35 | Средняя | Средняя | Угроза актуальна |
| Внедрение вирусов-компаньонов | 5 | Низкая(Y2=2) | 0.35 | Средняя | Средняя | Угроза актуальна |
| Внедрение вирусов-червей | 5 | Низкая(Y2=2) | 0.35 | Средняя | Средняя | Угроза актуальна |
| Внедрение Link-вирусов | 5 | Низкая(Y2=2) | 0.35 | Средняя | Средняя | Угроза актуальна |
| Внедрение макровирусов | 5 | Низкая(Y2=2) | 0.35 | Средняя | Средняя | Угроза актуальна |
| Угрозы, реализуемые посредством сокрытия информации в аудиоконтейнерах | 5 | Низкая(Y2=2) | 0.35 | Средняя | Низкая | Угроза не актуальна |
| Угрозы, реализуемые посредством сокрытия информации в текстовых контейнерах | 5 | Низкая(Y2=2) | 0.35 | Средняя | Низкая | Угроза не актуальна |
| Угрозы, реализуемые посредством сокрытия информации в графических контейнерах | 5 | Низкая(Y2=2) | 0.35 | Средняя | Низкая | Угроза не актуальна |
| Сбой системы электроснабжения | 5 | Низкая(Y2=2) | 0.35 | Средняя | Средняя | Угроза актуальна |
| Стихийное бедствие | 5 | Низкая(Y2=2) | 0.35 | Средняя | Средняя | Угроза актуальна |

**РАЗРАБОТАНО:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ответственный за организацию обработки и обеспечение безопасности персональных данных |  |  |  | А.Е. Запольских |
|  |  | (подпись, дата) |  | (инициалы, фамилия) |

**С документом ознакомлен (а):**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Директор  |  |  |  | О.А. Бурухина  |
|  |  | (подпись, дата) |  | (инициалы, фамилия) |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Администратор безопасности ИСПДн  |  |  |  |  | Н.А. Блохин |
|  |  |  | (подпись, дата) |  | (инициалы, фамилия) |