**4. МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПДН**

**Порядок определения актуальных угроз безопасности персональных данных в информационных системах персональных данных**

Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для ПДн. Подход к составлению перечня актуальных угроз состоит в следующем.

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

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн

Исходная степень защищенности определяется следующим образом.

1. ИСПДн имеет ***высокий*** уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню «высокий» (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные – среднему уровню защищенности (положительные решения по второму столбцу).

2. ИСПДн имеет ***средний*** уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний» (берется отношение суммы положительные решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные – низкому уровню защищенности.

3. ИСПДн имеет ***низкую*** степень исходной защищенности, если не выполняются условия по пунктам 1 и 2.

При составлении перечня актуальных угроз безопасности ПДн каждой степени исходной защищенности 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.

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показателя, 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 Y2 , 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

*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 (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.

Затем осуществляется выбор из общего (предварительного) перечня угроз безопасности тех, которые относятся к актуальным для данной ИСПДн.

**4.1. Модель угроз безопасности ПДн, обрабатываемых в ИСПДн «Active Directory»**

**4.1.1. Уровень исходной защищённости ИСПДн**

Документом ФСТЭК России «Методика актуализации угроз ПДн» вводится обобщенный показатель уровня исходной защищенности ИСПДн, зависящий от технических и эксплуатационных характеристик ИСПДн. (коэффициент Y1).

В соответствии с заданными критериями оценки определяется уровень исходной защищенности ИСПДн «Active Directory».

|  |  |  |
| --- | --- | --- |
| Технические и эксплуатационные характеристики ИСПДн | | Уровень защищённости |
| 1. По территориальному размещению | корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации | Средний |
| 2. По наличию соединения с сетями общего пользования | ИСПДн, имеющая многоточечный выход в сеть общего пользования | Низкий |
| 3. По встроенным (легальным) операциям с записями баз персональных данных | чтение, поиск | Высокий |
| 4. По разграничению доступа к персональным данным | ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект ПДн | Средний |
| 5. По наличию соединений с другими базами ПДн иных ИСПДн | ИСПДн, в которой используется одна база ПДн, принадлежащая организации-владельцу данной ИСПДн | Высокий |
| 6. По уровню обобщения (обезличивания) ПДн | ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации | Средний |
| 7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки | ИСПДн, не предоставляющая никакой информации | Высокий |

По совокупности полученных результатов уровень исходной защищенности ИСПДн «Active Directory» оценивается как средний, поскольку не менее 70% характеристик ИСПДн (86%) соответствуют уровню «средний» или «высокий».

Согласно «Методики актуализации угроз ПДн» ФСТЭК России, коэффициент исходной защищенности ИСПДн «Active Directory» и Y1=5.

4.2.2. Описание угроз безопасности ПДн

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Класс угроз** | **Источник угроз** | | **Способ реализации** | | | | | | **Объект воздействия** | | **Нарушаемые свойства ИБ** | | | **Вероятность реализации** | | |
| Угрозы 1-го типа | | | | | | | | | | | | | | | | |
| 1. Угроза НСД с применением стандартных функций операционной системы | Внутренний нарушитель | | Доступ в операционную среду ИСПДн, реализуемый при помощи эксплуатации НДВ (уязвимостей системного ПО), осуществляемый при физическом доступе к ИСПДн или средствам ввода информации в ИСПДн | | | | | | Технические средства ИСПДн (АРМ  пользователей, сервера приложений/БД ИСПДн) Программные средства ИСПДн: ОС | | Нарушение  конфиденциальности,  целостности и  доступности ПДн | | | Средняя вероятность | | |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Используется лицензионное системное ПО надежных производителей. 2. На серверах, функционирующих под управлением ОС Windows, устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости. 3. Доступ в помещения, где расположены сервера, ограничен и контролируется. 4. Идентификация и аутентификация осуществляется по доменным учетным записям и паролям. 5. Обеспечивается разграничение доступа пользователей к ИСПДн. Факторы, повышающие вероятность реализации угрозы: 6. Не осуществляется настройка безопасности ОС на серверах. 7. Для аутентификации используются слабые пароли, настройки парольной политики не соответствуют лучшим международным практикам. В частности, длина пароля недостаточна (6 символов), срок действия пароля не ограничен и не осуществляется блокирование учетной записи после некоторого количества неуспешных попыток ввода пароля. | | | | | | | | | | | | |
| 2. Угроза НСД с применением специально  созданных для  этого программ | Внутренний нарушитель Внешний нарушитель | | Реализуется путем эксплуатации НДВ в системном ПО (известных уязвимостей) | | | | | | Технические средства ИСПДн: сервера приложений/БД ИСПДн  Программные средства ИСПДн: ОС | | Нарушение  конфиденциальности,  целостности и доступности ПДн | | | Средняя вероятность | | |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Используется лицензионное системное ПО надежных производителей. 2. На серверах, функционирующих под управлением ОС Windows, устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости. 3. На серверах установлено антивирусное ПО. Осуществляется регулярное обновление антивирусного ПО. Управление антивирусным ПО осуществляется централизовано. 4. Идентификация и аутентификация осуществляется по доменным учетным записям и паролям. 5. Обеспечивается разграничение доступа пользователей к ИСПДн. Факторы, повышающие вероятность реализации угрозы: 6. Не осуществляется настройка безопасности ОС на серверах. 7. Для аутентификации используются слабые пароли, настройки парольной политики не соответствуют лучшим международным практикам. В частности, длина пароля недостаточна (6 символов), срок действия пароля не ограничен и не осуществляется блокирование учетной записи после некоторого количества неуспешных попыток ввода пароля. | | | | | | | | | | | | |
| 3. Угрозы типа  «Отказ в обслуживании», в том числе  использование известных уязвимостей в ПО | Внешний нарушитель | | Реализуется путем эксплуатации уязвимостей НДВ в системном ПО | | | | | | Программные средства ИСПДн - ОС | | Нарушение  доступности ПДн | | | Низкая вероятность | | |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Используется лицензионное системное ПО надежных производителей. 2. При осуществлении взаимодействия с сетью Интернет используются средства межсетевого экранирования. 3. В ЛВС используются только коммутаторы и маршрутизаторы (хабы не используются). 4. На серверах, функционирующих под управлением ОС Windows, устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости. | | | | | | | | | | | | |
| 4. Угрозы удаленного  запуска  приложений, в том числе:  - распространение файлов, содержащих несанкционированный исполняемый код;  - переполнение буфера приложений серверов;  - использование возможностей удаленного управления системой | Внешний нарушитель | | Реализуется путем эксплуатации уязвимостей, вызванных  наличием НДВ в системном ПО | | | | | | Программные средства ИСПДн: ОС | | Нарушение  конфиденциальности, целостности и  доступности ПДн | | | Низкая вероятность | | |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Используется лицензионное системное ПО надежных производителей. 2. На серверах, функционирующих под управлением ОС Windows, устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.   На серверах установлено антивирусное ПО. Осуществляется регулярное обновление антивирусного ПО. Управление антивирусным ПО осуществляется централизовано.   1. При осуществлении взаимодействия с сетью Интернет используются средства межсетевого экранирования. 2. Обеспечивается разграничение доступа пользователей к ИСПДн. | | | | | | | | | | | | |
| Угрозы 2-го типа | | | | | | | | | | | | | | | | |
| 5. Угроза НСД с применением стандартных функций прикладного ПО | | Внутренний нарушитель | | | | Доступ в операционную среду ИСПДн, реализуемый при помощи эксплуатации НДВ  (уязвимостей прикладного ПО), осуществляемый при физическом доступе к ИСПДн или средствам ввода информации в ИСПДн | | | | Технические средства ИСПДн (АРМ  пользователей, сервера приложений/БД ИСПДн) Программные средства ИСПДн: ППО, СУБД | | Нарушение  конфиденциальности, целостности и  доступности ПДн | | | Средняя вероятность | |
|  | | Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Используется лицензионное ПО надежных производителей. 2. На серверах и рабочих станциях пользователей устанавливаются обновления и патчи для прикладного ПО, сервисов и служб, которые закрывают известные и новые уязвимости. 3. Доступ в помещения, где расположены сервера, ограничен и контролируется. 4. Идентификация и аутентификация осуществляется по доменным учетным записям и паролям.   Обеспечивается разграничение доступа пользователей к ИСПДн.  Факторы, повышающие вероятность реализации угрозы:  1. Для аутентификации используются слабые пароли, настройки парольной политики не соответствуют лучшим международным практикам. В частности, длина пароля недостаточна (6 символов), срок действия пароля не ограничен и не осуществляется блокирование учетной записи после некоторого количества неуспешных попыток ввода пароля. | | | | | | | | | | | | |  | |
| 6. Угроза НСД с применением  специально  созданных для  этого программ | Внутренний нарушитель Внешний нарушитель | | Реализуется путем эксплуатации  НДВ в прикладном ПО  (известных уязвимостей) | | | | | | Технические средства ИСПДн: сервера приложений/БД ИСПДн  Программные средства ИСПДн: ППО, СУБД | | Нарушение  конфиденциальности, целостности и  доступности ПДн | | | Средняя вероятность | | |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Используется лицензионное ПО надежных производителей. 2. На серверах и рабочих станциях пользователей устанавливаются обновления и патчи для прикладного ПО, сервисов и служб, которые закрывают известные и новые уязвимости. 3. На серверах установлено антивирусное ПО. Осуществляется регулярное обновление антивирусного ПО. Управление антивирусным ПО осуществляется централизовано. 4. Идентификация и аутентификация осуществляется по доменным учетным записям и паролям. 5. Обеспечивается разграничение доступа пользователей к ИСПДн.   Факторы, повышающие вероятность реализации угрозы: для аутентификации используются слабые пароли, настройки парольной политики не соответствуют лучшим международным практикам. В частности, длина пароля недостаточна (6 символов), срок действия пароля не ограничен и не осуществляется блокирование учетной записи после некоторого количества неуспешных попыток ввода пароля. | | | | | | | | | | | | |
| 7. Угрозы типа  «Отказ в обслуживании», в том числе  использование известных уязвимостей в ПО | Внешний нарушитель | | Реализуется путем эксплуатации уязвимостей НДВ в прикладном ПО | | | | | | Программные средства ИСПДн ППО, СУБД | | Нарушение  доступности ПДн | | | Низкая вероятность | | |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Используется лицензионное ПО надежных производителей. 2. При осуществлении взаимодействия с сетью Интернет используются средства межсетевого экранирования. 3. В ЛВС используются только коммутаторы и маршрутизаторы (хабы не используются). 4. На серверах, функционирующих под управлением ОС Windows, устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.   Факторы, повышающие вероятность реализации угрозы: средства анализа защищенности не используются | | | | | | | | | | | | |
| 8. Угрозы удаленного  запуска  приложений, в том числе:  - распространение файлов, содержащих несанкционированный исполняемый код; - переполнение буфера приложений серверов;  - использование возможностей удаленного управления системой | Внешний нарушитель | | Реализуется путем эксплуатации уязвимостей, вызванных  наличием НДВ в прикладном ПО | | | | | | Программные средства ИСПДн: ППО, СУБД | | Нарушение  конфиденциальности, целостности и  доступности  ПДн | | | Низкая вероятность | | |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Используется лицензионное системное ПО надежных производителей. 2. На серверах, функционирующих под управлением ОС Windows, устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости. 3. На серверах установлено антивирусное ПО. Осуществляется регулярное обновление антивирусного ПО. Управление антивирусным ПО осуществляется централизовано. 4. При осуществлении взаимодействия с сетью Интернет используются средства межсетевого экранирования. 5. Обеспечивается разграничение доступа пользователей к ИСПДн.   Факторы, повышающие вероятность реализации угрозы: средства анализа защищенности не используются | | | | | | | | | | | | |
| Угрозы 3-го типа | | | | | | | | | | | | | | | | |
| 9. Угрозы утечки акустической (речевой) информации | | Внешний нарушитель | | | Перехват акустической (речевой) информации с использованием аппаратуры, регистрирующей акустические и вибро-акустические волны, а также электромагнитные излучения, оптические и электрические сигналы, модулированные информативным акустическим сигналом.  Перехват акустической (речевой) информации с использованием специальных электронных устройств съема речевой  информации | | | Технические  средства обработки  ПДн, ВТСС,  строительные конструкции, инженерно-технические коммуникации, персонал ИСПДн | | | | | Нарушение конфиденциальности ПДн | | | Маловероятная вероятность |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы: речевой (акустический) ввод/вывод информации в данной ИСПДн не предусмотрен. | | | | | | | | | | | | | |
| 10. Угрозы утечки видовой информации | | Внешний нарушитель Внутренний нарушитель | | Просмотр ПДн с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео и буквенно-цифровой информации | | | Технические средства обработки ПДн, помещения, персонал ИСПДн | | | | | | Нарушение конфиденциальности ПДн | | | Низкая вероятность |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:  1. Доступ в помещения, где расположены сервера, ограничен и контролируется.  2. Средства отображения информации в серверных помещениях защищены от визуального просмотра. | | | | | | | | | | | | | |
|  | | Внешний нарушитель | | | | Просмотр ПДн с помощью специальных электронных устройств съема, внедренных в служебных помещениях или скрытно используемых физическими лицами при посещении ими служебных помещений | Технические средства обработки ПДн, помещения, персонал ИСПДн | | | | | | Нарушение конфиденциальности ПДн | | | Низкая вероятность |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы: доступ в помещения, где расположены сервера, ограничен и контролируется. | | | | | | | | | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 11. Угрозы  утечки информации по каналам ПЭМИН | Внешний нарушитель | Перехват техническими средствами побочных (не связанных с прямым функциональным значением элементов ИСПДн) информативных  электромагнитных полей электрических сигналов, возникающих при обработке ПДн техническими средствами  ИСПДн | Инженернотехнические коммуникации (цепи электропитания, шины заземления и т.д.) Института  ВТСС (средства и системы охранной и пожарной сигнализации и  т.д.) Института  Линии связи и передачи данных Технические  средства обработки  ПДн (рабочие станции, сервера и  т.д.) | Нарушение конфиденциальности ПДн | Низкая вероятность |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы: при обработке информации, основную опасность при реализации угрозы утечки по каналам ПЭМИН представляют утечки из-за наличия электромагнитных излучений монитора. Ввиду большого числа рабочих станция и другого оборудования, выделение необходимой информации из общей среды представляется маловероятным. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 12. Угрозы модификации базовой системы ввода/вывода (BIOS), перехвата управления  загрузкой,  перехвата или подбора паролей или идентификаторов, а также использование технологических паролей BIOS | Внутренний нарушитель Внешний нарушитель | Реализуются с использованием отчуждаемых носителей информации. Осуществляются перехват паролей или идентификаторов, модификация программного обеспечения базовой системы ввода-вывода (BIOS), перехват управления загрузкой с целью изменения необходимой технологической информации для получения НСД в операционную среду ИСПДн | Программные средства ИСПДн: базовая система ввода-вывода (BIOS).  Технические средства ИСПДн | Нарушение  конфиденциальности,  целостности и  доступности  ПДн | Низкая вероятность |
| Применяемые защитные меры, снижающие вероятность угроз: доступ в помещения, где расположены сервера, ограничен и контролируется.  Факторы, повышающие вероятность реализации угрозы: аутентификация пользователей при доступе к BIOS не осуществляется. | | | |