**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.

4.1.2. 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. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 13. Угроза  НСД с применением стандартных функций операционной системы, СУБД, прикладной программы | Внутренний нарушитель Внешний нарушитель | Доступ в операционную среду ИСПДн с использованием программных и программно-аппаратных средств ввода/вывода рабочих станций (серверов), входящих в состав ИСПДн, осуществляемый при физическом доступе к ИСПДн или средствам ввода информации в ИСПДн | Программные средства ИСПДн: ОС, СУБД, прикладные системы. Технические средства ИСПДн | Нарушение  конфиденциальности,  целостности и  доступности ПДн | Высокая 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. 5. Пароли в открытом виде в ИСПДн не хранятся. 6. Обеспечивается разграничение доступа пользователей к ИСПДн. 7. Пользователи не обладают административными правами на серверах.   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. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 14. Угроза НСД с  Применением специально  созданных для  этого программ | Внутренний нарушитель Внешний нарушитель | Реализуется путем эксплуатации вредоносного кода с целью получения доступа к программным средствам ИСПДн | Технические средства ИСПДн: сервера приложений/БД ИСПДн  Программные средства ИСПДн: ППО, СУБД | Нарушение  конфиденциальности,  целостности и  доступности ПДн | Высокая 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. Пользователи не обладают административными правами на серверах.   Факторы, повышающие вероятность реализации угрозы:   1. Не осуществляется настройка безопасности ОС на рабочих станциях пользователей. 2. Излишнее ПО, не являющееся необходимым для реализации бизнес-процессов, не удалено с рабочих станций пользователей. 3. 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. 4. Пользователи обладают правами локальных администраторов на своих рабочих станциях. 5. При покидании пользователем рабочего места не производится блокировка АРМ. | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 15. Угроза утечки информации путем преднамеренного  копирования доступных ПДн на неучтенные (в том числе отчуждаемые) носители, а также печать неучтенных  копий документов с  ПДн на принтерах | Внутренний нарушитель Внешний нарушитель | Копирование выгруженной ИСПДн информации на отчуждаемые носители | Из | Программные средства ИСПДн: ОС, СУБД, прикладные системы. | Нарушение конфиденциальности ПДн | Средняя вероятность |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Доступ в помещения, где расположены сервера, ограничен и контролируется. 2. Обеспечивается разграничение доступа пользователей к ИСПДн. 3. Идентификация и аутентификация осуществляется по доменным учетным записям и паролям.   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. | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 16. Угроза внедрения  вредоносных  программ с  использованием съемных носителей, а также в связи с подключением стороннего оборудования (компьютеров,  КПК, смартфонов, телефонов, фотоаппаратов,  видеокамер,  флэш-дисков и иных устройств, в том числе имеющих выход в беспроводные сети связи) | Внутренний нарушитель Внешний нарушитель | Доступ в операционную среду ИСПДн с использованием вредоносных программ, загруженных с использованием съемных носителей | Программные средства ИСПДн: ОС, СУБД,  прикладные системы, технические средства ИСПДн. | Нарушение  конфиденциальности,  целостности и  доступности ПДн | Низкая вероятность |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Доступ в помещения, где расположены сервера, ограничен и контролируется. 2. Обеспечивается разграничение доступа пользователей к ИСПДн. 3. Идентификация и аутентификация осуществляется по доменным учетным записям и паролям. 4. На серверах установлено антивирусное ПО. Осуществляется регулярное обновление антивирусного ПО. Управление антивирусным ПО осуществляется централизовано.   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. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 17. Угроза  «Анализа сетевого трафика» | Внутренний нарушитель Внешний нарушитель | Использование программ анализаторов пакетов (снифферов) для перехвата ПДн (и иной конфиденциальной информации), а также для перехвата идентификаторов и паролей удаленного доступа (к сетевым службам) | Технические средства ИСПДн (каналы связи) | Нарушение конфиденциальности:  исследование характеристик сетевого трафика, перехват передаваемых  данных, в том числе идентификаторов и паролей пользователей | Высокая вероятность |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Доступ в помещения, где расположены сервера, ограничен и контролируется. 2. Обеспечивается разграничение доступа к кроссовому оборудованию. 3. В ЛВС используются только коммутаторы и маршрутизаторы (хабы не используются). 4. При осуществлении взаимодействия с сетью Интернет используются средства межсетевого экранирования. 5. При обмене информацией между серверными площадками Института, передаваемый трафик защищается при помощи технологии VPN. 6. При осуществлении удаленного доступа траффик защищается при помощи технологии VPN. 7. При использовании беспроводных сетей осуществляется идентификация/аутентификация пользователей по доменным учетным записям с помощью протокола Radius. Из гостевой сети WiFi возможен доступ только в сеть Интернет.   Факторы, повышающие вероятность реализации угрозы:  1. Излишнее ПО, не являющееся необходимым для реализации бизнес-процессов, не удалено с рабочих станций пользователей и серверов.  2. 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. Пользователи обладают правами локальных администраторов на своих рабочих станциях. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 18. Угроза сканирования сети | Внутренний нарушитель Внешний нарушитель | Передача запросов сетевым службам хостов ИСПДн и анализ ответов на них с целью:   * инвентаризации сетевых ресурсов (поиск узлов сети, определение их адресов, типов ОС); * выявления активных сетевых служб, используемых портов, версий программ (уязвимых); * выявления неиспользуемых, но установленных сетевых служб   (уязвимых) | Технические средства ИСПДн (каналы связи), программные средства ИСПДн | Нарушение конфиденциальности:  определение протоколов, доступных портов сетевых служб, идентификаторов соединений, активных сетевых  сервисов,  идентификаторов и паролей пользователей. Нарушение доступности:  возможен отказ в обслуживании сканируемых сетевых сервисов | Высокая вероятность |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Обеспечивается разграничение доступа к кроссовому оборудованию. 2. Доступ в помещения, где расположены сервера, ограничен и контролируется. 3. При осуществлении взаимодействия с сетью Интернет используются средства межсетевого экранирования. 4. Права пользователей ограничены и не распространяются на установку ПО, а также отключение или изменение настроек СЗИ на серверах. 5. При использовании беспроводных сетей осуществляется идентификация/аутентификация пользователей по доменным учетным записям с помощью протокола Radius. Из гостевой сети WiFi возможен доступ только в сеть Интернет.   Факторы, повышающие вероятность реализации угрозы:   1. Не используется система обнаружения/предотвращения вторжений. 2. Излишнее ПО, не являющееся необходимым для реализации бизнес-процессов, не удалено с рабочих станций пользователей и серверов. 3. Пользователи обладают правами локальных администраторов на своих рабочих станциях. 4. 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. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 19. Угроза выявления паролей | Внутренний нарушитель Внешний нарушитель | Перебор паролей (в том числе с использованием  специализированного ПО), установка вредоносных программ для перехвата паролей, подмена доверенного объекта сети (IPspoofing), перехват пакетов (sniffing). Взлом перехваченных в сети защищенных паролей (хэш) | Технические средства ИСПДн (каналы связи), программные средства ИСПДн | Нарушение  конфиденциальности,  целостности и доступности ПДн: выполнение любого  действия,  связанного с получением несанкционированного доступа | Высокая вероятность |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. На серверах установлено антивирусное ПО. Осуществляется регулярное обновление антивирусного ПО. Управление антивирусным ПО осуществляется централизовано. 2. При осуществлении взаимодействия с сетью Интернет используются средства межсетевого экранирования. 3. Аутентификационные данные пользователей передаются в защищенном виде. 4. Пароли хранятся в виде хэш-сумм. 5. Осуществляются идентификация и аутентификация по доменным учетным записям и паролям. 6. При осуществлении удаленного доступа траффик защищается при помощи технологии VPN.   При использовании беспроводных сетей осуществляется идентификация/аутентификация пользователей по доменным учетным записям с помощью протокола Radius. Из гостевой сети WiFi возможен доступ только в сеть Интернет.  Факторы, повышающие вероятность реализации угрозы:   1. Не используется система обнаружения/предотвращения вторжений. 2. Излишнее ПО, не являющееся необходимым для реализации бизнес-процессов, не удалено с рабочих станций пользователей и серверов. 3. Пользователи обладают правами администратора на рабочих станциях. 4. 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. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 20. Угроза навязывания ложного маршрута сети | Внутренний нарушитель Внешний нарушитель | Несанкционированное использование протоколов маршрутизации (RIP, OSPF, LSP, EIGRP) и управления сетью (ICMP, SNMP) для внесения изменений в маршрутно-адресные таблицы | Технические средства ИСПДн | Нарушение  конфиденциальности,  целостности и доступности: несанкционированное изменение маршрутно-адресных данных, анализ и модификация передаваемых данных, навязывание ложных сообщений | Средняя вероятность |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Обеспечивается разграничение доступа к кроссовому оборудованию. 2. Доступ в помещения, где расположены сервера, ограничен и контролируется. 3. В ЛВС используются только коммутаторы и маршрутизаторы (хабы не используются). 4. При использовании беспроводных сетей осуществляется идентификация/аутентификация пользователей по доменным учетным записям с помощью протокола Radius. Из гостевой сети WiFi возможен доступ только в сеть Интернет.   Факторы, повышающие вероятность реализации угрозы:   1. Не используется система обнаружения/предотвращения вторжений. 2. Излишнее ПО, не являющееся необходимым для реализации бизнес-процессов, не удалено с рабочих станций пользователей и серверов.   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. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 21. Угроза внедрения ложного объекта  сети | Внутренний нарушитель Внешний нарушитель | Перехват поискового запроса в протоколах удаленного поиска (ARP, DNS, WINS) - в сетях со стеком протоколов TCP/IP, и выдача на него ложного ответа, использование которого приводит к требуемому изменению в маршрутно- адресных данных | Технические средства ИСПДн | Нарушение  конфиденциальности,  целостности и доступности ПДн: перехват и просмотр трафика, несанкционированный доступ к  сетевым ресурсам, навязывание ложной информации | Средняя вероятность |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:  1. Обеспечивается разграничение доступа к кроссовому оборудованию.  2. Доступ в помещения Института, где расположены рабочие станции пользователей, ограничен и контролируется. В случае удаленного использования рабочих станций за границами контролируемой зоны Института ответственность за безопасность рабочих станций возложена на работников.  3. В ЛВС используются только коммутаторы и маршрутизаторы (хабы не используются).  4. При использовании беспроводных сетей осуществляется идентификация/аутентификация пользователей по доменным учетным записям с помощью протокола Radius. Из гостевой сети WiFi возможен доступ только в сеть Интернет.  Факторы, повышающие вероятность реализации угрозы:  1. Не используется система обнаружения/предотвращения вторжений.  2. Излишнее ПО, не являющееся необходимым для реализации бизнес-процессов, не удалено с рабочих станций пользователей.  3. 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. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 22. Угрозы типа «Отказ в обслуживании», в том числе:   * частичное использование   ресурсов;   * полное исчерпание ресурсов; * нарушение   логической связности между техническими  средствами  ИСПДн;   * использование ошибок в   программах | Внутренний нарушитель | - привлечение части ресурсов  ИСПДн на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований к времени обработки запросов;   * исчерпание ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником   (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание);   * передача нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных или идентификационной и аутентификационной информации;   передача пакетов с нестандартными атрибутами или имеющих длину, превышающую максимально допустимый размер | Технические средства ИСПДн (каналы связи), программные средства ИСПДн | Нарушение доступности за счет:  - снижения  Пропускной способности каналов связи, производительности сетевых устройств; снижение производительности серверных приложений; - невозможности передачи сообщений из-за отсутствия доступа к среде передачи, отказ в установлении соединения,  отказ в предоставлении сервиса;  - невозможности передачи, сообщений (получения услуг) из-за  отсутствия корректных маршрутно-адресных данных; нарушения  работоспособности сетевых устройств | Средняя 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. 5. На серверах установлено антивирусное ПО. Осуществляется регулярное обновление антивирусного ПО. Управление антивирусным ПО осуществляется централизовано. 6. Права пользователей на серверах ограничены.   Факторы, повышающие вероятность реализации угрозы:   1. Излишнее ПО, не являющееся необходимым для реализации бизнес-процессов, не удалено с рабочих станций пользователей и серверов. 2. Не используется система обнаружения/предотвращения вторжений. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 23. 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 некорректными настройками операционной системы, СУБД, сетевых сервисов, прикладного ПО.  Использование скрытых компонентов ("троянских" программ) либо штатных средств управления и администрирования компьютерных сетей. | Технические средства ИСПДн (каналы связи), программные средства ИСПДн | 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. Обеспечивается разграничение доступа пользователей к ИСПДн. 5. При осуществлении взаимодействия с сетью Интернет используются средства межсетевого экранирования. 6. При осуществлении удаленного доступа траффик защищается при помощи технологии VPN. 7. Пользователи не обладают административными правами на серверах.   Факторы, повышающие вероятность реализации угрозы: излишнее ПО, не являющееся необходимым для реализации бизнес-процессов, не удалено с рабочих станций пользователей и серверов. | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Внешний нарушитель. Внутренний нарушитель | Реализуется путем эксплуатации web-уязвимостей | Программные средства ИСПДн | Нарушение  конфиденциальности,  целостности и  доступности ПДн | Маловероятная угроза |  |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:  в ИСПДн web-технологии не используются. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 24. Угроза внедрения по сети вредоносных программ | Внутренний нарушитель | Реализуется через почтовый или файловый обмен. Запись кода вредоносного ПО в код других программ с целью получения управления при запуске зараженных файлов, создание файлов-двойников для легального  ПО, копирование кода вредоносной программы в каталоги для последующего  запуска пользователем | Программные средства ИСПДн | Нарушение конфиденциальности,  целостности и  доступности ПДн | Низкая вероятность |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Обеспечивается разграничение доступа пользователей к ИСПДн. 2. На серверах установлено антивирусное ПО. Осуществляется регулярное обновление антивирусного ПО. Управление антивирусным ПО осуществляется централизовано. 3. На серверах, функционирующих под управлением ОС Windows, устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Внешний нарушитель, Внутренний нарушитель | Реализуется путем эксплуатации уязвимостей, вызванных некорректными настройками операционной системы, СУБД  или сетевых сервисов | Программные средства ИСПДн | Нарушение  конфиденциальности,  целостности и  доступности ПДн | Средняя вероятность |
|  | Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Обеспечивается разграничение доступа пользователей к ИСПДн. 2. На серверах рабочих станциях установлено антивирусное ПО. Осуществляется регулярное обновление антивирусного ПО. Управление антивирусным ПО осуществляется централизовано. 3. На серверах, функционирующих под управлением ОС Windows, устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости. 4. При осуществлении удаленного доступа траффик защищается при помощи технологии VPN.   Факторы, повышающие вероятность реализации угрозы: не осуществляется настройка безопасности ОС на рабочих станциях пользователей и серверах. | | | |

##### 4.1.3. Определение актуальности угроз безопасности ПДн

Результаты определения актуальности угроз безопасности ПДн, обрабатываемых в ИСПДн:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Класс угроз** | **Вероятность реализации** | **Y2** | **Коэффициент реализуемости угрозы Y** | **Возможность реализации** | **Опасность** | **Актуальность** |
| **Угрозы первого типа** |  |  | |  | |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Угроза НСД с применением стандартных функций операционной системы | Средняя вероятность | 5 | 0,5 | Средняя | Низкая | Неактуальная |
| Угроза НСД с применением специально созданных для этого программ | Средняя вероятность | 5 | 0,5 | Средняя | Низкая | Неактуальная |
| Угрозы типа «Отказ в обслуживании», в том числе использование известных уязвимостей в ПО | Низкая вероятность | 2 | 0,35 | Средняя | Низкая | Неактуальная |
| Угрозы удаленного запуска приложений, в том числе:  ­ распространение файлов, содержащих несанкционированный исполняемый код;  ­ переполнение буфера приложенийсерверов;  ­ использование возможностей удаленного управления системой. | Низкая вероятность | 2 | 0,35 | Средняя | Низкая | Неактуальная |
| **Угрозы второго типа** | | | | | | |
| Угроза НСД с применением стандартных функций прикладного ПО | Средняя вероятность | 5 | 0,5 | Средняя | Низкая | Неактуальная |
| Угроза НСД с применением специально созданных для этого программ | Средняя вероятность | 5 | 0,5 | Средняя | Низкая | Неактуальная |
| Угрозы типа «Отказ в обслуживании», в том числе использование известных уязвимостей в ПО | Низкая вероятность | 2 | 0,35 | Средняя | Низкая | Неактуальная |
| Угрозы удаленного запуска приложений, в том числе:  ­ распространение файлов, содержащих несанкционированный исполняемый код; | Низкая вероятность | 2 | 0,35 | Средняя | Низкая | Неактуальная |
| ­ переполнение буфера приложенийсерверов;  ­ использование возможностей удаленного управления системой. |  |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Угрозы третьего типа** | | | | | | |
| Угрозы утечки акустической (речевой) информации | Маловероятн  ая угроза | 0 | 0,25 | Низкая | Низкая | Неактуальная |
| Угрозы утечки видовой информации | Низкая вероятность | 2 | 0,35 | Средняя | Низкая | Неактуальная |
| Низкая вероятность | 2 | 0,35 | Средняя | Низкая | Неактуальная |
| Угрозы утечки информации по каналам  ПЭМИН | Низкая вероятность | 2 | 0,35 | Средняя | Низкая | Неактуальная |
| Угрозы модификации базовой системы ввода/вывода (BIOS), перехвата управления загрузкой, перехвата или подбора паролей или идентификаторов, а также использование технологических паролей BIOS | Низкая вероятность | 2 | 0,35 | Средняя | Низкая | Неактуальная |
| Угроза НСД с применением стандартных функций операционной системы, СУБД, прикладной программы | Высокая вероятность | 10 | 0,75 | Высокая | Низкая | Актуальная |
| Угроза НСД с применением специально созданных для этого программ | Высокая вероятность | 10 | 0,75 | Высокая | Низкая | Актуальная |
| Угроза утечки информации путем преднамеренного копирования доступных ПДн на неучтенные (в том числе отчуждаемые) носители, а также печать неучтенных копий документов с | Средняя вероятность | 5 | 0,5 | Средняя | Низкая | Неактуальная |
| ПДн на принтерах |  |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Угроза внедрения вредоносных программ с использованием съемных носителей, а также в связи с подключением стороннего оборудования (компьютеров, КПК, смартфонов, телефонов, фотоаппаратов, видеокамер, флэш-дисков и иных устройств, в том числе имеющих выход в беспроводные сети связи) | Низкая вероятность | 2 | 0,35 | Средняя | Низкая | Неактуальная |
| Угроза «Анализа сетевого трафика» | Высокая вероятность | 10 | 0,75 | Высокая | Низкая | Актуальная |
| Угроза сканирования сети | Высокая вероятность | 10 | 0,75 | Высокая | Низкая | Актуальная |
| Угроза выявления паролей | Высокая вероятность | 10 | 0,75 | Высокая | Низкая | Актуальная |
| Угроза навязывания ложного маршрута сети | Средняя вероятность | 5 | 0,5 | Средняя | Низкая | Неактуальная |
| Угроза внедрения ложного объекта сети | Средняя вероятность | 5 | 0,5 | Средняя | Низкая | Неактуальная |
| Угрозы типа «Отказ в обслуживании», в том числе:  ­ частичное использование ресурсов;  ­ полное исчерпание ресурсов;  ­ нарушение логической связности между техническим средствами ИСПДн;  ­ использование ошибок в программах. | Средняя вероятность | 5 | 0,5 | Средняя | Низкая | Неактуальная |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Угрозы удаленного запуска приложений, в том числе:  ­ распространение файлов, содержащих несанкционированный исполняемый код;  ­ переполнение буфера приложенийсерверов;  ­ использование возможностей удаленного управления системой. | Средняя вероятность | 5 | 0,5 | Средняя | Низкая | Неактуальная |
| Маловероятн  ая угроза | 0 | 0,25 | Низкая | Низкая | Неактуальная |
| Угроза внедрения по сети вредоносных программ | Низкая вероятность | 2 | 0,35 | Средняя | Низкая | Неактуальная |
| Средняя вероятность | 5 | 0,5 | Средняя | Низкая | Неактуальная |