**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ**

**РОССИЙСКОЙ ФЕДЕРАЦИИ**

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА ПО ДИСЦИПЛИНЕ

«ПРОЕКТНАЯ ДЕЯТЕЛЬСНОТЬ»

на тему:

**Разработка частной модели угроз безопасности ПДн для ИСПДН**

Куратор проекта: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / , \_\_\_\_\_\_\_\_\_\_\_\_ /

*подпись* *ФИО, уч. звание и степень*

Студент: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /Абрамов А.C, 171-361 /

*подпись* *ФИО, группа*

Студент: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /Кондратьева А.В, 171-361 /

*подпись* *ФИО, группа*

Студент: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /Цапин Д.М, 171-361 /

*подпись* *ФИО, группа*

Студент: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /Иванова Н.С, 171-361 /

*подпись* *ФИО, группа*

Москва 2020

Оглавление

[Введение 3](#_Toc43585887)

Индивидуальные планы………………………………………………………………5

[1. Типы угроз безопасности ПДн 6](#_Toc43585888)

[1.1 Угрозы утечки информации по техническим каналам 6](#_Toc43585889)

[1.2 Угрозы утечки акустической (речевой) информации 6](#_Toc43585890)

[1.3 Угрозы утечки видовой информации 6](#_Toc43585891)

[1.4 Угрозы утечки информации по каналам ПЭМИН 7](#_Toc43585892)

[1.5 Угрозы НСД 8](#_Toc43585893)

[1.6 Угрозы НСД, связанные с действиями нарушителей, имеющих доступ к ИСПДн. 8](#_Toc43585894)

[1.7 Угрозы внедрения по сети вредоносных программ (программно-математического воздействия) 15](#_Toc43585895)

[2. Модель угроз безопасности ИСПДН 17](#_Toc43585896)

[3. ИСПДн «Active Directory». 19](#_Toc43585897)

[4. Модель угроз безопасности ПДн, обрабатываемых в ИСПДн «Active Directory» 20](#_Toc43585898)

[4.1. Уровень исходной защищённости ИСПДн 20](#_Toc43585899)

[4.2. Описание угроз безопасности ПДн 22](#_Toc43585900)

[4.3. Определение актуальности угроз безопасности ПДн 47](#_Toc43585901)

[5. ИСПДн «1C: Бухгалтерия 8.3». 52](#_Toc43585902)

[6. ИСПДн «1C: ЗИК 8.3» 54](#_Toc43585903)

[7. ИСПДн «distance.learning.ru» 56](#_Toc43585904)

[8. Модель угроз безопасности ПДн, обрабатываемых в ИСПДн «distance.learning.ru» и «Портал ДПО» 58](#_Toc43585905)

[8.1 Уровень исходной защищённости ИСПДн 58](#_Toc43585906)

[8.2 Описание угроз безопасности ПДн 60](#_Toc43585907)

[9. ИСПДн «Рабочие станции пользователей» 98](#_Toc43585908)

[10. Модель угроз безопасности ПДн, обрабатываемых в ИСПДн «Рабочие станции пользователей» 101](#_Toc43585909)

[10.1 Уровень исходной защищённости ИСПДн 101](#_Toc43585910)

[10.2 Описание угроз безопасности ПДн 102](#_Toc43585911)

[10.3. Определение актуальности угроз безопасности ПДн 130](#_Toc43585912)

Заключение………………………………………………………………………….133

# Введение

Тема проекта-реализация модели угроз безопасности ПДн при их обработке в ИСПДН.

Практический результат работы над проектом-модель угроз,разработанная в соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной заместителем директора ФСТЭК России, на основе «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных».  
 При формировании настоящей Модели угроз безопасности персональных данных использовались следующие нормативно-правовые документы:

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

- Постановление Правительства Российской Федерации № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- Приказ ФСТЭК России «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденное приказом ФСБ России;

- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора ФСТЭК России;

- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора ФСТЭК России;

- Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденные руководством 8 Центра ФСБ России 31.03.2015 № 149/7/2/6-432;

Наш проект был направлен на изучение того,каковы возможные угрозы безопасности ПДн субъектов,насколько они реализуемы и какова их актуализация,так как в век информационных технологий безопасность ПДн субъектов крайне важна.

Участники проекта-студенты направления 10.03.01 “Информационная безопасность”.

Роли участников проекта:

Абрамов А.С:

Изучение составляющих следующих ИСПдн:

* Рабочие станции пользователей,
* 1C Бухгалтерия 8.3,
* 1С ЗИК 8.3,
* Подготовка их описания,составление техническую документацию к проекту

### Кондратьева А.В.

Изучение составляющих следующих ИСПдн:

* Active Directory и distance.learning.ru.
* Подготовка их описания,ведение и оформление сайта к проекту.

### Цапин Д.М.

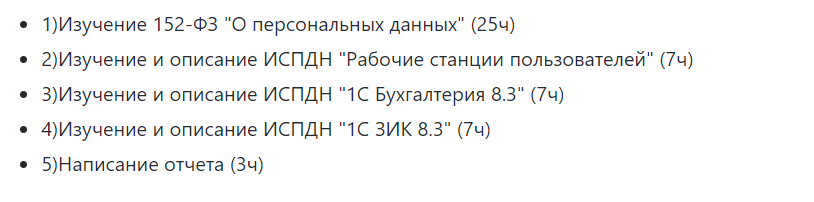
* Определение основных видов угроз безопасности персональных данных,
* Разработка модели угроз безопасности ПДн,обрабатываемых в ИСПДН:
* «Рабочие станции пользователей» и Портал ДПО

### Иванова Н.С.

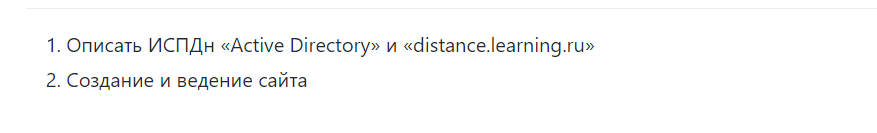
* Определение методики рассчета коэффициента исходной защищенности типовой ИСПДН
* Разработка модели угроз безопасности ПДн,обрабатываемых в ИСПДН:
* Active Directory и distance.learning.ru

Индивидуальные планы участников

Абрамов А.С



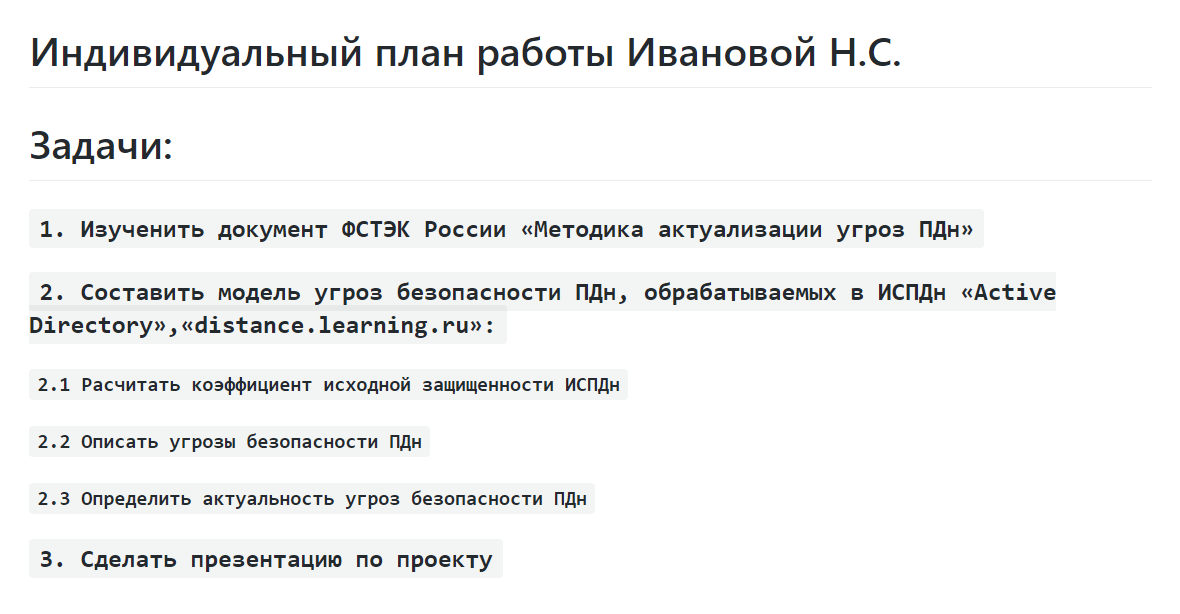
Кондратьева А.В



Цапин Д.М



Иванова Н.С



# 1. Типы угроз безопасности ПДн

Угрозы безопасности ПДн классифицируются по типу используемой уязвимости ИСПДн. Выделяются следующие типы угроз:

- угрозы, связанные с наличием недокументированных (не декларированных) возможностей в системном программном обеспечении, используемом в ИСПДн (угрозы 1-го типа);

- угрозы, связанные с наличием недокументированных (не декларированных) возможностей в прикладном программном обеспечении, используемом в ИСПДн (угрозы 2-го типа);

- угрозы, не связанные с наличием недокументированных (не декларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИСПДн (угрозы 3-го типа).

## 1.1 Угрозы утечки информации по техническим каналам

При обработке ПДн в ИСПДн возможно возникновение угроз безопасности ПДн за счет реализации следующих технических каналов утечки информации:

1. Угрозы утечки акустической (речевой) информации.
2. Угрозы утечки видовой информации.
3. Угрозы утечки информации по каналам ПЭМИН.

## 1.2 Угрозы утечки акустической (речевой) информации

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, при обработке ПДн в ИСПДн, возможно при наличии функций голосового ввода ПДн

* ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн. Утечка акустической (речевой) информации может быть осуществлена:
* с помощью аппаратных закладок;
* за счет съема виброакустических сигналов;
* за счет излучений, модулированных акустическим сигналом (микрофонный эффект и ВЧ облучение);
* за счет оптического излучения, модулированного акустическим

сигналом.

## 1.3 Угрозы утечки видовой информации

Угрозы утечки видовой информации реализуются за счет просмотра 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, входящих в состав ИСПДн.

Кроме этого, просмотр (регистрация) ПДн возможен с использованием специальных электронных устройств съема, внедренных в служебных помещениях или скрытно используемых физическими лицами при посещении ими служебных помещений.

Необходимым условием осуществления просмотра (регистрации) ПДн является наличие прямой видимости между средством наблюдения и носителем ПДн.

Утечка видовой информации может быть осуществлена:

* за счет удаленного просмотра экранов дисплеев и других средств отображения информации;
* с помощью видео аппаратных закладок.

## 1.4 Угрозы утечки информации по каналам ПЭМИН

Возникновение угрозы ПДн по каналам ПЭМИН возможно за счет перехвата техническими средствами побочных (не связанных с прямым

функциональным значением элементов ИСПДн) информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПДн техническими средствами ИСПДн.

Генерация информации, содержащей ПДн и циркулирующей в технических средствах ИСПДн в виде электрических информативных сигналов, обработка и передача указанных сигналов в электрических цепях технических средств ИСПДн сопровождается побочными электромагнитными излучениями, которые могут распространяться за пределы служебных помещений в зависимости от мощности излучений и размеров ИСПДн.

Регистрация ПЭМИН осуществляется с целью перехвата информации, циркулирующей в технических средствах, осуществляющих обработку ПДн

(средствах вычислительной техники, информационно-вычислительных комплексах и сетях, средствах и системах передачи, приема и обработки ПДн, средствах и системах звукозаписи, звукоусиления, звуковоспроизведения, переговорных и телевизионных устройствах, средствах изготовления, тиражирования документов и других технических средствах обработки речевой, графической, видео - и буквенно-цифровой информации).

Для регистрации ПЭМИН используется аппаратура в составе радиоприемных устройств и оконечных устройств восстановления информации.

Утечка информации по каналам ПЭМИН может быть осуществлена:

* за счет побочных электромагнитных излучений электронно-вычислительной техники;
* за счет наводок по цепям питания;
* за счет радиоизлучений, модулированных информационным сигналом.

## 1.5 Угрозы НСД

Угрозы НСД в ИСПДн с применением программных и программно-аппаратных средств реализуются при осуществлении несанкционированного, в том числе случайного доступа, в результате которого осуществляется нарушение конфиденциальности (копирование, несанкционированное распространение), целостности (уничтожение, изменение) и доступности (блокирование) ПДн, и включают в себя:

* 1. Угрозы НСД, связанные с действиями нарушителей, имеющих доступ
* ИСПДн.
  1. Угрозы, связанные с реализацией протоколов сетевого взаимодействия, реализуемые внутри распределенной сети.
  2. Угрозы внедрения (в том числе по сети) вредоносных программ (программно-математического воздействия).

## 1.6 Угрозы НСД, связанные с действиями нарушителей, имеющих доступ к ИСПДн.

Данные угрозы могут быть реализованы нарушителем в случае получения физического доступа к ИСПДн или, по крайней мере, к средствам ввода информации в ИСПДн. При этом можно выделить следующие угрозы:

1. Угрозы, реализуемые в ходе загрузки операционной системы.

Эти угрозы безопасности информации направлены на перехват паролей или идентификаторов, модификацию программного обеспечения базовой системы ввода-вывода (BIOS), перехват управления загрузкой с изменением необходимой технологической информации для получения НСД в операционную среду ИСПДн. Чаще всего такие угрозы реализуются с использованием отчуждаемых носителей информации.

1. Угрозы, реализуемые после загрузки операционной среды, независимо от того, какая прикладная программа запускается пользователем.

Эти угрозы, как правило, направлены на выполнение непосредственно несанкционированного доступа к информации. При получении доступа в операционную среду нарушитель может воспользоваться как стандартными функциями операционной системы (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) или какой-либо прикладной программой общего пользования (например, системы управления базами данных), так и специально созданными для выполнения несанкционированного доступа программами, например:

* программами просмотра и модификации реестра;
* программами поиска текстов в текстовых файлах по ключевым словам

копирования;

* специальными программами просмотра и копирования записей в базах

данных;

* программами быстрого просмотра графических файлов, их редактирования или копирования;
* программами поддержки возможностей реконфигурации программной среды (настройки ИСПДн в интересах нарушителя) и др.

Кроме того, к данным угрозам необходимо отнести угрозы утечки информации путем копирования ее на съемные носители.

1. Угрозы, реализуемые после загрузки операционной среды, реализация которых определяется тем, какая из прикладных программ запускается пользователем, или фактом запуска любой из прикладных программ. Большая часть таких угроз представляет собой угрозы внедрения вредоносных программ.

Угрозы, связанные с реализацией протоколов сетевого взаимодействия, реализуемые внутри распределенной сети

Можно выделить следующие угрозы, реализуемые с использованием протоколов сетевого взаимодействия, реализуемые внутри распределенной сети:

1. Угрозы «Анализа сетевого трафика».

Эта угроза реализуется с помощью специальной программы-анализатора пакетов (sniffer), перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль, а также конфиденциальная информация.

1. Угрозы сканирования сети.

Сущность процесса реализации угрозы заключается в передаче запросов сетевым службам хостов ИСПДн и анализе ответов от них с целью выявления используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов, подбора идентификаторов и паролей пользователей.

1. Угрозы выявления паролей.

Цель реализации угрозы состоит в получении НСД путем преодоления парольной защиты. Злоумышленник может реализовывать угрозу с помощью целого ряда методов, таких как простой перебор, перебор с использованием специальных словарей, установка вредоносной программы для перехвата пароля, подмена доверенного объекта сети (IP-spoofing) и перехват пакетов (sniffing). В основном для реализации угрозы используются специальные программы, которые пытаются получить доступ к хосту путем последовательного подбора паролей. В случае успеха злоумышленник может создать для себя «проход» для будущего доступа, который будет действовать, даже если на хосте изменить пароль доступа.

1. Угрозы навязывания ложного маршрута сети.

Данная угроза реализуется путем несанкционированного изменения маршрутно-адресных данных. Возможность навязывания ложного маршрута обусловлена недостатками, присущими алгоритмам маршрутизации (в частности, из-за проблемы идентификации сетевых управляющих устройств), в результате

чего можно попасть, например, на хост или в сеть злоумышленника, где можно войти в операционную среду технического средства в составе ИСПДн. Реализация угрозы основывается на несанкционированном использовании протоколов маршрутизации (RIP, OSPF, LSP) и управления сетью (ICMP, SNMP) для внесения изменений в маршрутно-адресные таблицы. При этом нарушителю необходимо послать от имени сетевого управляющего устройства (например, маршрутизатора) управляющее сообщение.

1. Угрозы внедрения ложного объекта сети.

Эта угроза основана на использовании недостатков алгоритмов удаленного поиска. В случае если объекты сети изначально не имеют адресной информации друг о друге, используются различные протоколы удаленного поиска (например, SAP в сетях Novell NetWare; ARP, DNS, WINS в сетях со стеком протоколов TCP/IP), заключающиеся в передаче по сети специальных запросов и получении на них ответов с искомой информацией. При этом существует возможность перехвата нарушителем поискового запроса и выдачи на него ложного ответа, использование которого приведет к требуемому изменению маршрутно-адресных данных. В дальнейшем весь поток информации, ассоциированный с объектом-жертвой, будет проходить через ложный объект сети.

1. Угрозы типа «Отказ в обслуживании».

Эти угрозы основаны на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, когда операционная система оказывается не в состоянии обрабатывать поступающие пакеты.

Может быть выделено несколько разновидностей таких угроз:

* скрытый отказ в обслуживании, вызванный привлечением части ресурсов ИСПДн на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований к времени обработки запросов. Примерами реализации угроз подобного рода могут служить: направленный шторм эхо-запросов по протоколу ICMP (Pingflooding), шторм запросов на установление TCP-соединений (SYN-flooding), шторм запросов к FTP-серверу;
* явный отказ в обслуживании, вызванный полным исчерпанием ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание), при котором легальные запросы не могут быть переданы через сеть из-за недоступности среды передачи либо получают отказ в обслуживании ввиду переполнения очередей запросов, дискового пространства памяти и т.д. Примерами угроз данного типа могут служить шторм широковещательных ICMP-эхо-запросов (Smurf), направленный шторм (SYN-flooding), шторм сообщений почтовому серверу (Spam); явный отказ в обслуживании, вызванный нарушением логической связности между техническими средствами ИСПДн при передаче нарушителем

управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных (например, ICMP Redirect Host, DNS-flooding) или

идентификационной и аутентификационной информации; явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа «Land», «Tear Drop», «Bonk», «Nuke», «UDP-bomb») или имеющих длину, превышающую максимально допустимый размер (угроза типа «Ping Death»), что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

Результатом реализации данной угрозы может стать нарушение работоспособности соответствующей службы предоставления удаленного доступа

* ПДн в ИСПДн, передача с одного адреса такого количества запросов на подключение к техническому средству в составе ИСПДн, какое максимально может «вместить» трафик (направленный «шторм запросов»), что влечет за собой переполнение очереди запросов и отказ одной из сетевых служб или полная остановка ИСПДн из-за невозможности системы заниматься ничем другим, кроме обработки запросов;
  1. Угрозы удаленного запуска приложений.

Угроза заключается в стремлении запустить на хосте ИСПДн различные предварительно внедренные вредоносные программы:

* программы-закладки;
* вирусы;
* «сетевые шпионы» и т.д.

Основная цель внедренных вредоносных программ – нарушение конфиденциальности, целостности, доступности информации и полный контроль за работой хоста. Кроме того, возможен несанкционированный запуск прикладных программ пользователей для несанкционированного получения необходимых нарушителю данных, для запуска управляемых прикладной программой процессов и др.

Выделяют три подкласса данной угрозы:

1) распространение файлов, содержащих несанкционированный исполняемый код. Типовые угрозы этого подкласса основываются на активизации распространяемых файлов при случайном обращении к ним. Примерами таких файлов могут служить: файлы, содержащие исполняемый код в виде макрокоманд (документы Microsoft Word, Excel и т.п.); html-документы, содержащие исполняемый код в виде элементов ActiveX, Java-апплетов, интерпретируемых скриптов (например, тексты на JavaScript); файлы, содержащие исполняемые коды программ. Для распространения файлов могут использоваться службы электронной почты, передачи файлов, сетевой файловой системы;

2) удаленный запуск приложения путем переполнения буфера приложений-серверов. При угрозах этого подкласса используются недостатки программ, реализующих сетевые сервисы (в частности, отсутствие контроля за

переполнением буфера). Настройкой системных регистров иногда удается переключить процессор после прерывания, вызванного переполнением буфера, на исполнение кода, содержащегося за границей буфера. Примером реализации такой угрозы может служить внедрение широко известного «вируса Морриса»;

3) удаленный запуск приложения путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками, либо используемыми штатными средствами. При угрозах этого подкласса нарушитель использует возможности удаленного управления системой, предоставляемые скрытыми компонентами (например, «троянскими» программами типа BackOrifice, NetBus), либо штатными средствами управления и администрирования компьютерных сетей (Landesk Management Suite, Managewise, BackOrifice и т. п.). В результате их использования удается добиться удаленного контроля над станцией в сети.

## 1.7 Угрозы внедрения по сети вредоносных программ (программно-математического воздействия)

Программно-математическое воздействие - это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

* скрывать признаки своего присутствия в программной среде компьютера;
* обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;
* разрушать (искажать произвольным образом) код программ в оперативной памяти;
* выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирования, уничтожения, блокирования и т.п.);
* сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);
* искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

Вредоносные программы могут быть внесены (внедрены) как преднамеренно, так и случайно в программное обеспечение, используемое в ИСПДн, в процессе его разработки, сопровождения, модификации и настройки. Кроме этого, вредоносные программы могут быть внесены в процессе эксплуатации ИСПДн с внешних носителей информации или посредством

сетевого взаимодействия как в результате НСД, так и случайно пользователями ИСПДн.

Вредоносные программы основаны на использовании уязвимостей различного рода программного обеспечения и разнообразных сетевых технологий, обладают широким спектром возможностей и могут действовать во всех видах программного обеспечения.

Наличие в ИСПДн вредоносных программ может способствовать возникновению скрытых, в том числе нетрадиционных каналов доступа к информации, позволяющих вскрывать, обходить или блокировать защитные механизмы, предусмотренные в системе, в том числе парольную защиту.

Источники угроз безопасности ПДн

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Источниками угроз НСД в ИСПДн могут быть:

* нарушитель;
* носитель вредоносной программы;
* аппаратная закладка.

Категории нарушителей безопасности ПДн

Целью возможного нарушителя является нарушение характеристик безопасности защищаемых объектов путем модификации, разрушения или блокирования программных и технических средств, хищения и ознакомления с защищаемой информацией, а также навязывания ложной информации, или побуждения к принятию неверных решений.

Контролируемой зоной является:

* территория офиса, включая помещения общего доступа, предназначенные для работы с клиентами;
* серверное помещение, расположенное в Институте.



Рабочие станции пользователей, расположенные в помещениях общего доступа, находятся под постоянным визуальным наблюдением работников Института, в связи с этим доступ посторонних лиц к рабочим стациям ограничен.

* точки зрения наличия возможности постоянного или разового доступа в контролируемую зону, в которой размещены технические средства ИСПДн, все нарушители могут быть отнесены к следующим двум категориям:
* категория I: внешние нарушители - физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещаются технические средства ИСПДн Института, а также права легального физического доступа к техническим средствам ИСПДн;
* категория II: внутренние нарушители - физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещаются технические средства ИСПДн Института.

Под внешним нарушителем информационной безопасности рассматривается нарушитель, не имеющий непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны.

# 2. Модель угроз безопасности ИСПДН

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.

# 3. ИСПДн «Active Directory».

3.1 Общее описание

Назначение системы: автоматизация настроек пользовательской среды.

Статус системы: в промышленной эксплуатации.

Пользователи: доступ в систему работников Института не осуществляется.

##### Обрабатываемые в системе персональные данные

|  |  |
| --- | --- |
| Категория субъектов ПДн | Перечень персональных данных |
|
| Работники Института | * ФИО, * подразделение, * адрес электронной почты. |

Количество записей около 5000.

3.2 Описание технологии функционирования и архитектуры системы

Сопровождение: администрирование ОС и ППО – Управление информатизации. Структура ИСПДн:

ИС состоит из следующих компонентов: контроллеров домена.

Контроллеры домена находятся на каждой территориальной площадке Института. Сводная информация по компонентам системы представлена в таблице ниже:

|  |  |  |  |
| --- | --- | --- | --- |
| Компонент ИСПДн | Установленное ПО | |  |
| ОС | СУБД | ППО |
| Контроллер домена | Windows  Server 2012 Standart | Microsoft  Active  Directory | - |

3.3 Описание механизмов и средств защиты

Регистрация событий: осуществляется на уровне операционной системы серверов. Регистрируются такие события, как вход и выход пользователя.

Аутентификация:

Для аутентификации используется доменная пара логин\пароль.

Средствами контроллера домена настроена и контролируется следующая парольная политика:

­ минимальная длина пароля – 6 символов;

­ пароль должен содержать как буквы, так и цифры;

­ срок действия пароля неограничен;

­ независимо от количества неуспешных попыток ввода пароля в систему, блокировка учетной записи не осуществляется.

Антивирусная защита:

В Институте на серверах установлено антивирусное ПО Касперский Endpoint Protection 10. Данное антивирусное ПО имеет клиент-серверную архитектуру, при которой управление функционированием антивирусного ПО осуществляется централизованно.

Обновление антивирусных баз и модулей производится ежедневно. Контроль целостности обновлений и программной части ведется встроенными средствами антивирусного ПО.

# 4. Модель угроз безопасности ПДн, обрабатываемых в ИСПДн «Active Directory»

## 4.1. 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. 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. | | | |

## 4.3. 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 |

# 5. ИСПДн «1C: Бухгалтерия 8.3».

5.1 Общее описание

Назначение системы: автоматизация бухгалтерского и налогового учета

Пользователи: работники Института

Обрабатываемые в системе персональные данные:

|  |  |
| --- | --- |
| Категория субъектов ПДн | Перечень персональных данных |
| Работники Института | * ФИО; * табельный номер; * серия и номер паспорта; * дата выдачи паспорта и выдавшая его организация; * общий трудовой стаж; * ИНН; * адрес регистрации; * адрес проживания; * номера телефонов; * сведения о доходах. * сумма к перечислению. |
| Сотрудники контрагентов Института | * ФИО; * серия и номер паспорта; * дата выдачи паспорта и выдавшая его организация; * дата и место рождения; * ИНН; * сумма к перечислению. |

5.2 Описание технологии функционирования и архитектуры системы

Сопровождение: администрирование ОС и ППО – Управление информатизации.

Структура ИСПДн:

ИС состоит из сервера БД и приложений.

Работники получают доступ к системе при помощи клиентского ПО («толстый» клиент), установленного на их рабочих станциях.

Сводная информация по компонентам системы представлена в таблице ниже:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Компонент ИСПДн | Установленное ПО | | | Количество | Размещение |
| ОС | СУБД | ПО |
| Сервер БД и  приложений  (виртуальный) | Windows  Server2012  Standart | Microsoft  SQL  Server  2012 | \_ | 1 | Территориальные площадки университета, распложенные в г. Москва и филиалах. (серверное помещение) |

5.3 Описание механизмов и средств защиты

Регистрация событий: регистрируются такие события, как вход и выход пользователя, изменение документов.

Аутентификация:

Для аутентификации в системе используются локальные учетные записи. Средствами ППО настроена и контролируется следующая парольная политика:

* минимальная длина пароля – 6 символов;
* пароль должен содержать как буквы, так и цифры;
* срок действия пароля неограничен;
* независимо от количества неуспешных попыток ввода пароля в систему, блокировка учетной записи не осуществляется.

Антивирусная защита:

В Институте на серверах установлено антивирусное ПО Касперский Endpoint Protection 10. Данное антивирусное ПО имеет клиент-серверную архитектуру, при которой управление функционированием антивирусного ПО осуществляется централизованно.

Обновление антивирусных баз и модулей производится ежедневно. Контроль целостности обновлений и программной части ведется встроенными средствами антивирусного ПО.

# 6. ИСПДн «1C: ЗИК 8.3»

6.1 Общее описание

Назначение системы: автоматизация кадрового учета

Пользователи: работники Института

Обрабатываемые в системе персональные данные:

|  |  |
| --- | --- |
| Категория субъектов ПДн | Перечень персональных данных |
| Работники Института | * ФИО; * табельный номер; * серия и номер паспорта; * дата выдачи паспорта и выдавшая его организация; * общий трудовой стаж; * ИНН; * адрес регистрации; * адрес проживания; * номера телефонов; * сведения о доходах. * реквизиты; * сумма к перечислению. |
| Сотрудники контрагентов Института | * ФИО; * серия и номер паспорта; * дата выдачи паспорта и выдавшая его организация; * дата и место рождения; * ИНН; * реквизиты; * сумма к перечислению. |
| Обущающиеся | * ФИО; * учебная группа; * серия и номер паспорта; * дата выдачи паспорта и выдавшая его организация; * реквизиты; * сумма к перечислению. |

Обьем (кол-во записей) около 50000

6.2 Описание технологии функционирования и архитектуры системы Сопровождение: администрирование ОС и ППО – Управление информатизации.

Структура ИСПДн:

ИС состоит из сервера БД и приложений.

Работники получают доступ к системе при помощи клиентского ПО («толстый» клиент), установленного на их рабочих станциях.

Сводная информация по компонентам системы представлена в таблице ниже:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Компонент ИСПДн | Установленное ПО | | | Количество | Размещение |
| ОС | СУБД | ПО |
| Сервер БД и  приложений  (виртуальный) | Windows  Server2012  Standart | Microsoft  SQL  Server  2012 | \_ | 1 | Территориальные площадки университета, распложенные в г. Москва и филиалах. (серверное помещение) |

6.3 Описание механизмов и средств защиты

Регистрация событий: регистрируются такие события, как вход и выход пользователя, изменение документов.

Аутентификация:

Для аутентификации в системе используются локальные учетные записи. Средствами ППО настроена и контролируется следующая парольная политика:

* минимальная длина пароля – 6 символов;
* пароль должен содержать как буквы, так и цифры;
* срок действия пароля неограничен;
* независимо от количества неуспешных попыток ввода пароля в систему, блокировка учетной записи не осуществляется.

Антивирусная защита:

В Институте на серверах установлено антивирусное ПО Касперский Endpoint Protection 10. Данное антивирусное ПО имеет клиент-серверную архитектуру, при которой управление функционированием антивирусного ПО осуществляется централизованно.

Обновление антивирусных баз и модулей производится ежедневно. Контроль целостности обновлений и программной части ведется встроенными средствами антивирусного ПО.

# 7. ИСПДн «distance.learning.ru»

7.1 Общее описание

Назначение системы: система управления обучением.

Пользователи:

* работники Института,
* гостевые учетные записи,
* обучающиеся.

Обрабатываемые в системе персональные данные

|  |  |
| --- | --- |
| Категория субъектов ПДн | Перечень персональных данных |
|
| Слушатели курсов | * ФИО, * изображение, * тип пользователя, * фотография, * страна и город проживания, * номер телефона, * идентификационные данные онлайн-мессенджеров, * индивидуальный номер, * учреждение(организация), * отдел, * адрес электронной почты, * адрес. |
| Преподаватели | * ФИО, * изображение, * тип пользователя, * фотография * страна и город проживания, * номер телефона, * адрес электронной почты, * должность, * идентификационные данные онлайн-мессенджеров, * учреждение(организация), * отдел, * адрес. |

Количество записей около 123000.

7.2 Описание технологии функционирования и архитектуры системы Сопровождение: администрирование ОС и ППО – Управление информатизации.

Структура ИСПДн:

1. Веб-сервер.

2. Сервер БД.

3. Сервер приложений.

Пользователи получают доступ к системе при веб-клиента, для доступа и передачи данных используется защищенный протокол https.

Система разработана на платформе с открытым кодом moodle.

Сводная информация по компонентам системы представлена в таблице ниже:

|  |  |  |  |
| --- | --- | --- | --- |
| Компонент ИСПДн | Установленное ПО | | |
| ОС | СУБД | ППО |
| Веб-сервер | Debian 8 | - | nginx |
| Сервер БД  (виртуальный) | Debian 8.3 | MySQL  5.46 | - |
| Сервер приложений  (виртуальный) | Ubuntu  12.04.5 | - | - |

Размещение в городе Москва.

* 1. Описание механизмов и средств защиты

Регистрация событий: регистрируются такие события, как вход и выход пользователя, изменение документов.

Аутентификация:

Для аутентификации в системе используются локальные учетные записи. Средствами ППО настроена и контролируется следующая парольная политика:

* минимальная длина пароля – 6 символов;
* пароль должен содержать как буквы, так и цифры;
* срок действия пароля неограничен;
* независимо от количества неуспешных попыток ввода пароля в систему, блокировка учетной записи не осуществляется.

Антивирусная защита:

В Институте на серверах установлено антивирусное ПО Касперский Endpoint Protection 10. Данное антивирусное ПО имеет клиент-серверную архитектуру, при которой управление функционированием антивирусного ПО осуществляется централизованно.

Обновление антивирусных баз и модулей производится ежедневно. Контроль целостности обновлений и программной части ведется встроенными средствами антивирусного ПО.

# 8. Модель угроз безопасности ПДн, обрабатываемых в ИСПДн «distance.learning.ru» и «Портал ДПО»

## 8.1 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 «Портал ДПО», «distance.learning.ru»

(коэффициент Y1).

|  |  |  |
| --- | --- | --- |
| Технические и эксплуатационные характеристики ИСПДн | | Защищенность |
| По территориальному  размещению | локальная ИСПДн, развернутая в пределах одного здания | Высокая |
| По наличию  соединения с сетями  общего пользования | ИСПДн, имеющая одноточечный  выход в сеть общего пользования | Средний |
| По встроенным  операциям с записями баз персональных данных | - чтение, поиск;  - запись, удаление, сортировка;  - модификация, передача | Низкий |
| По разграничению  доступа к персональным данным | ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем  ИСПДн, либо субъект ПДн | Средний |
| По наличию соединений с другими Базами ПДн иных ИСПДн | Интегрированная  (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем используемых баз) | Низкий |
| 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 |
| По объему ПДн,  которые  предоставляются  сторонним | ИСПДн, не предоставляющая никакой информации | Высокий |

По совокупности полученных результатов уровень исходной защищенности ИСПДн «Портал ДПО», оценивается как средний, поскольку не менее 70% характеристик ИСПДн (71%) соответствуют уровню «средний» или «высокий».

Согласно «Методики актуализации угроз ПДн» ФСТЭК России, коэффициент исходной защищенности ИСПДн «Портал ДПО», «distance.learning.ru» Y1=5.

## 8.2 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:**   1. Не осуществляется настройка безопасности ОС на серверах. 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. Требования парольной политики не настроены и не контролируются | | | | | | | | | | | | |
| 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 | | | 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. Идентификация и аутентификация осуществляется по доменным учетным записям и паролям. 5. Обеспечивается разграничение доступа пользователей к ИСПДн.   **Факторы, повышающие вероятность реализации угрозы:**   1. Не осуществляется настройка безопасности ОС на серверах. 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. Требования парольной политики не настроены и не контролируются | | | | | | | | | | | | |
| 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 | | | Средняя 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.   **Факторы,повышающие вероятность реализации угрозы:**   1. На части серверов не 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 | | | Средняя вероятность | | |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Используется лицензионное системное ПО надежных производителей. 2. На части серверов устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости. 3. При осуществлении взаимодействия с сетью Интернет используются средства межсетевого экранирования. 4. Обеспечивается разграничение доступа пользователей к ИСПДн.   **Факторы,повышающие вероятность реализации угрозы:**   1. На части серверов не устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости. | | | | | | | | | | | | |
| 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 части серверов 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. Обеспечивается разграничение доступа пользовтелей к ИСПДн   **Факторы, повышающие вероятность реализации угрозы:**   1. На части серверов не устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости. 2. Требования парольной политики не настроены и не контролируются | | | | | | | | | | | | |  | |
| 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 части серверов устанавливаются обновления и патчи для прикладного ПО, сервисов и служб, которые закрывают известные и новые уязвимости. 3. Идентификация и аутентификация осуществляется по локальным учетным записям и паролям. 4. Обеспечивается разграничение доступа пользователей к ИСПДн.   **Факторы, повышающие вероятность реализации угрозы:**   1. На части серверов не устанавливаются обновления и патчи для прикладного ПО, сервисов и служб, которые закрывают известные и новые уязвимости. 2. Требования парольной политики не настроены и не контролируются | | | | | | | | | | | | |
| 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 | | | 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 части серверов устанавливаются обновления и патчи для прикладного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.   **Факторы, повышающие вероятность реализации угрозы:**   1. На части серверов не устанавливаются обновления и патчи для прикладного ПО, сервисов и служб, которые закрывают известные и новые уязвимости. 2. 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 | | | Средняя вероятность | | |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Используется лицензионное системное ПО надежных производителей. 2. На части серверов устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости. 3. При осуществлении взаимодействия с сетью Интернет используются средства межсетевого экранирования. 4. Обеспечивается разграничение доступа пользователей к ИСПДн.   **Факторы, повышающие вероятность реализации угрозы:**   1. На части серверов не устанавливаются обновления и патчи для прикладного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.      1. 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 | Инженерно-технические 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  нарушите ль  Внешний  нарушите  ль | | 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  доступности ПДн | и | | Высокая вероятность |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:  1. Используется лицензионное ПО надежных производителей.  2. На части серверов 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. 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:  1. На части серверов не устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.  2. Требования парольной политики не настроены и не контролируются. | | | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 14. Угроза НСД с применением  специально созданных  для этого программ | Внутренний  нарушитель | Реализуется путем эксплуатации вредоносного кода с целью получения доступа к программным средствам ИСПДн | Технические средства ИСПДн: сервера приложений/БД | 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 части серверов устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости. 3. Идентификация и аутентификация пользователей при входе в ОС на рабочих станциях осуществляется по доменным учетным записям и паролям. 4. Пользователи не обладают административными правами на серверах.   Факторы, повышающие вероятность реализации угрозы:   1. На части серверов не устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости. 2. Антивирусное ПО на серверах, функционирующих под управлением ОС семейства Linux не применяется. 3. Излишнее ПО, не являющееся необходимым для реализации бизнес-процессов, не удалено с рабочих станций пользователей и серверов. 4. Требования парольной политики не настроены и не контролируются.   Пользователи обладают правами локальных администраторов на своих рабочих станциях. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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 | Внутренн ий  нарушите ль  Внешний нарушитель | Копирование выгруженной из  ИСПДн информации на  отчуждаемые носители | Программные средства ИСПДн:  ОС, СУБД, прикладные системы. | Нарушение конфиденциальн ости 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 пользователей осуществляется по локальным учетным записям и паролям.  4. Пользователи не обладают административными правами на серверах. Факторы, повышающие вероятность реализации угрозы: требования парольной политики не настроены и не контролируются. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 16. Угроза внедрения  вредоносных  программ с  использованием съемных носителей, а также в связи с  подключением стороннего оборудования (компьютеров, КПК, смартфонов, телефонов, фотоаппаратов, видеокамер, флэшдисков 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 | 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 пользователей осуществляется по локальным учетным записям и паролям. 4. Пользователи не обладают административными правами на серверах. Факторы, повышающие вероятность реализации угрозы: 5. Требования парольной политики не настроены и не контролируются. 6. Антивирусное ПО на серверах, функционирующих под управлением ОС семейства Linux не применяется | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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. Пользователи не обладают административными правами на серверах.   Факторы, повышающие вероятность реализации угрозы:   1. Излишнее ПО, не являющееся необходимым для реализации бизнес-процессов, не удалено с рабочих станций пользователей и серверов. 2. Доступ пользователей осуществляется по незащищенному протоколу http | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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. Пользователи не обладают административными правами на серверах. Факторы, повышающие вероятность реализации угрозы: 5. Не используется система обнаружения/предотвращения вторжений. 6. Излишнее ПО, не являющееся необходимым для реализации бизнес-процессов, не удалено с рабочих станций пользователей и серверов.   Пользователи обладают правами локальных администраторов на своих рабочих станциях. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 19. Угроза выявления паролей | Внутренн ий  нарушите ль  Внешний  нарушите  ль | 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  конфиденциальн  ости,  целостности и доступности ПДн: выполнение любого  действия,  связанного с получением несанкциониров анного доступа | Высокая вероятность |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. При осуществлении взаимодействия с сетью Интернет используются средства межсетевого экранирования. 2. Пароли хранятся в виде хэш-сумм. 3. Осуществляются идентификация и аутентификация пользователей при входе в ОС по доменным учетным записям и паролям. 4. Пользователи не обладают административными правами на серверах. Факторы, повышающие вероятность реализации угрозы: 5. Не используется система обнаружения/предотвращения вторжений. 6. Антивирусное ПО на серверах, функционирующих под управлением ОС семейства Linux не применяется. 7. Излишнее ПО, не являющееся необходимым для реализации бизнес-процессов, не удалено с рабочих станций пользователей и серверов. 8. Требования парольной политики не настроены и не контролируются. 9. Пользователи обладают правами администратора на рабочих станциях.   Доступ пользователей осуществляется по незащищенному протоколу http. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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).   Факторы, повышающие вероятность реализации угрозы:   1. Не используется система обнаружения/предотвращения вторжений.   Излишнее ПО, не являющееся необходимым для реализации бизнес-процессов, не удалено с рабочих станций пользователей и серверов. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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. Доступ в серверное помещение ограничен и контролируется. 2. Обеспечивается разграничение доступа к кроссовому оборудованию. 3. В ЛВС используются только коммутаторы и маршрутизаторы (хабы не используются).   Факторы, повышающие вероятность реализации угрозы:   1. Не используется система обнаружения/предотвращения вторжений.   Излишнее ПО, не являющееся необходимым для реализации бизнес-процессов, не удалено с рабочих станций пользователей. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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  Внешний  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 | Высокая 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).   На части серверов устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.  Факторы, повышающие вероятность реализации угрозы:   1. Излишнее ПО, не являющееся необходимым для реализации бизнес-процессов, не удалено с рабочих станций пользователей и серверов. 2. Антивирусное ПО на серверах, функционирующих под управлением ОС семейства Linux не применяется. 3. На части серверов не устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.   Не используется система обнаружения/предотвращения вторжений. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 23. Угрозы удаленного запуска приложений, в том числе:   * распространение файлов, содержащих несанкционированный   исполняемый код;   * переполнение буфера приложений серверов; | 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 | Высокая вероятность |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Используется лицензионное системное ПО надежных производителей. 2. На части серверов устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости. 3. Обеспечивается разграничение доступа пользователей к ИСПДн. 4. При осуществлении взаимодействия с сетью Интернет используются средства межсетевого экранирования.   Факторы, повышающие вероятность реализации угрозы:   1. Излишнее ПО, не являющееся необходимым для реализации бизнес-процессов, не удалено с рабочих станций пользователей и серверов. 2. Антивирусное ПО на серверах, функционирующих под управлением ОС семейства Linux не применяется. 3. На части серверов устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.   Доступ пользователей осуществляется по незащищенному протоколу http. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Внешний нарушитель.  Внутренний  нарушитель | Реализуется путем эксплуатации web-уязвимостей | Программные средства ИСПДн | Нарушение  конфиденциальности,  целостности и  доступности ПДн | Высокая вероятность |
|  | Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. На части серверов устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости. 2. При осуществлении взаимодействия с сетью Интернет используются средства межсетевого экранирования.   Факторы, повышающие вероятность реализации угрозы:   1. Информационные системы построены при помощи открытых платформ, при разработке не учитывались требования безопасного программирования. Системы защиты класса WAF (web application firewall) не применяются. 2. Антивирусное ПО на серверах, функционирующих под управлением ОС семейства Linux не применяется. 3. На части серверов не устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости Информационные системы построены при помощи открытых платформ, при разработке не учитывались требования безопасного программирования. Системы защиты класса WAF (web application firewall) не применяются. 4. Доступ пользователей осуществляется по незащищенному протоколу http.   Отсканированные документы, которые прикрепляют кандидаты в систему «mioo.ru», доступны по внешней ссылке без авторизации любому лицу, знающему ее. | | | |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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 | Высокая вероятность |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Обеспечивается разграничение доступа пользователей к ИСПДн. 2. На части серверов устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.   Факторы, повышающие вероятность реализации угрозы:  1. На части серверов не устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.  3. Антивирусное ПО на серверах, функционирующих под управлением ОС семейства Linux не применяется. | | | |
| 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 | Высокая вероятность |
|  | Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:   1. Обеспечивается разграничение доступа пользователей к ИСПДн. 2. На части серверов устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.   Факторы, повышающие вероятность реализации угрозы:   1. Не осуществляется настройка безопасности ОС на рабочих станциях пользователей и серверах. 2. Антивирусное ПО на серверах, функционирующих под управлением ОС семейства Linux не применяется.   На части серверов не устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **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 | Средняя вероятность | 5 | 0,5 | Средняя | Низкая | Неактуальная |
| Угрозы удаленного запуска приложений, в том числе:  ­ распространение файлов, содержащих несанкционированный исполняемый код;  ­ переполнение буфера приложений серверов;  ­ использование возможностей удаленного управления системой. | Средняя вероятность | 5 | 0,5 | 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 | Средняя вероятность | 5 | 0,5 | Средняя | Низкая | Неактуальная |
| Угрозы удаленного запуска приложений, в том числе:  ­ распространение файлов, содержащих несанкционированный исполняемый код; | Средняя вероятность | 5 | 0,5 | Средняя | Низкая | Неактуальная |
| ­ переполнение буфера приложений серверов;  ­ 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 ПДн на принтерах | Средняя вероятность | 5 | 0,5 | Средняя | Низкая | Неактуальная |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 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) | Средняя вероятность | 5 | 0,5 | 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. | Высокая вероятность | 10 | 0,75 | Высокая | Низкая | Актуальная |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Угрозы удаленного запуска приложений, в том числе:  ­ распространение файлов, содержащих несанкционированный исполняемый код;  ­ переполнение буфера приложений, серверов;  ­ использование возможностей удаленного управления системой. | Высокая вероятность | 10 | 0,75 | Высокая | Низкая | Актуальная |
| Высокая вероятность | 10 | 0,75 | Высокая | Низкая | Актуальная |
| Угроза внедрения по сети вредоносных программ | Высокая вероятность | 10 | 0,75 | Высокая | Низкая | Актуальная |
| Высокая вероятность | 10 | 0,75 | Высокая | Низкая | Актуальная |

# 9. ИСПДн «Рабочие станции пользователей»

9.1 Общее описание

Назначение системы: автоматизация деятельности работников Московского Политеха.   
Статус системы: в эксплуатации.  
Пользователи: Работники Института.

Обрабатываемые в системе персональные данные:

|  |  |
| --- | --- |
| Категория субъектов ПДн | Перечень персональных данных |
| Работники Института | * ФИО; * табельный номер; * дата и место рождения; * пол; * место работы; * подразделение; * должность; * гражданство; * инвалидность; * серия и номер паспорта; * дата выдачи паспорта и выдавшая его организация; * общий трудовой стаж; * ИНН; * СНИЛС; * адрес регистрации; * адрес проживания; * номера телефонов; * семейное положение; * сведения о составе семьи; * сведения об образовании; * сведения о доходах. |
| Читатели лекций | * ФИО; * место работы; * должность; * номер телефона; * адрес электронной почты. |
| Сотрудники контрагентов Института | * ФИО; * серия и номер паспорта; * дата выдачи паспорта и выдавшая его организация, * дата и место рождения; * ИНН; * сумма к перечислению. |
| Обучающиеся | * ФИО; * пол; * день рождения; * номер зачетной книжки; * учебная группа; * номер телефона; * адрес электронной почты; * серия и номер паспорта; * дата выдачи паспорта и выдавшая его организация; * семейное положение. |
| Поступающие | * ФИО; * пол; * день рождения; * номер аттестата; * номер телефона; * адрес электронной почты; * серия и номер паспорта; * дата выдачи паспорта и выдавшая его организация; * семейное положение. |

Объем (количество записей): не более 10000

9.2 Описание технологии функционирования и архитектуры системы

Сопровождение: администрирование ОС и ППО – Управление информатизации.

Структура ИСПДн: система является многопользовательской и обеспечивает ролевое разграничение прав доступа пользователей. Система взаимодействует с ресурсами сети Интернет.

ИСПДн состоит из следующих компонентов:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Компонент ИСПДн | Установленное ПО | | | Количество | Размещение |
| ОС | СУБД | ПО |
| АРМ пользователей | Microsoft  Windows 7/10 | **\_** | 1C:Бухгалтерия 8.3  1C:Зарплата и  кадры 8.3,  Веб-браузер; | Не мнее 1000 рабочих станций, используемых для доступа к ИСПДН университета | Территориальные площадки университета, распложенные в г. Москва и филиалах. |

* 1. Описание механизмов и средств защиты

Регистрация событий: осуществляется регистрация событий на уровне операционной системы для рабочих станций.

Регистрируются такие события, как вход и выход пользователя.

Аутентификация:

Для аутентификации используется доменная пара логин\пароль.

Средствами контроллера домена настроена и контролируется следующая парольная политика:

* минимальная длина пароля – 6 символов;
* пароль должен содержать как буквы, так и цифры;
* срок действия пароля неограничен;
* независимо от количества неуспешных попыток ввода пароля в систему, блокировка учетной записи не осуществляется.

Антивирусная защита:

В Институте на всех АРМ установлено антивирусное ПО Касперский Endpoint Protection 10. Данное антивирусное ПО имеет клиент-серверную архитектуру, при которой управление функционированием антивирусного ПО осуществляется централизованно.

Обновление антивирусных баз и модулей производится ежедневно. Контроль целостности обновлений и программной части ведется встроенными средствами антивирусного ПО.

# 10. Модель угроз безопасности ПДн, обрабатываемых в ИСПДн «Рабочие станции пользователей»

## 10.1 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. «Рабочие станции пользователей» (коэффициент Y1).

* соответствии с заданными критериями оценки определяется уровень исходной защищенности ИСПДн «Рабочие станции пользователей»:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  | Уровень |  |  |
|  | Технические и эксплуатационные характеристики ИСПДн | | | | | | | | |  |  | защищеннос |  |  |
|  |  |  | ти |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | | | |  | |  |  | |  |  |  |  |  |
| 1. По территориальному | | | | | корпоративная | |  | распределенная | | |  | Средний | |  |
| размещению | | |  |  | ИСПДн, | охватывающая | | | многие | |  |  |
|  |  |  |  |  | подразделения одной организации | | | | | |  |  |  |  |
| 2. По | |  |  | наличию | ИСПДн, | имеющая | | одноточечный | | |  | Средний | |  |
| соединения | | | с | сетями | выход в сеть общего пользования | | | | | |  |  |
| общего пользования | | | | |  |  |  |  |  |  |  |  |  |  |
| 3. По | |  | встроенным | | - чтение, поиск; | | |  |  |  |  |  |  |  |
| (легальным) операциям с | | | | | - запись,удаление, сортировка; | | | |  |  |  | Низкий | |  |
| записями | | |  | баз | - модификация, передача | | | |  |  |  |  |
|  |  |  |  |  |  |  |
| персональных данных | | | | |  |  |  |  |  |  |  |  |  |  |
| 4. По | | разграничению | | | ИСПДн, к которой имеет доступ | | | | | |  |  |  |  |
| доступа к персональным | | | | | определенный | | перечень сотрудников | | | |  | Средний | |  |
| данным | |  |  |  | организации, являющейся владельцем | | | | | |  |  |
|  |  |  |  |  | ИСПДн, либо субъект ПДн | | | |  |  |  |  |  |  |
| 5. По | |  |  | наличию | Интегрированная | | |  | ИСПДн | |  |  |  |  |
| соединений | | | с | другими | (организация использует несколько баз | | | | | |  | Низкий | |  |
| базами | | ПДн | | иных | ПДн ИСПДн, при этом организация не | | | | | |  |  |
| ИСПДн | |  |  |  | является |  | владельцем | | всех | |  |  |  |  |
|  |  |  |  |  | используемых баз ПДн) | | | |  |  |  |  |  |  |
| 6. По уровню обобщения | | | | | ИСПДн, | в | которой | | данные | |  |  |  |  |
| (обезличивания) ПДн | | | | | обезличиваются только при передаче в | | | | | |  | Средний | |  |
|  |  |  |  |  | другие организации и не обезличены | | | | | |  |  |
|  |  |  |  |  | при предоставлении | | | пользователю в | | |  |  |  |  |
|  |  |  |  |  | организации | |  |  |  |  |  |  |  |  |
| 7. По | | объему | | ПДн, | ИСПДн, не предоставляющая никакой | | | | | |  | Высокий | |  |
| которые | |  |  |  | информации | |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |

По совокупности полученных результатов уровень исходной защищенности ИСПДн «Рабочие станции пользователей» оценивается как средний, поскольку не менее 70% характеристик ИСПДн (71%) соответствуют уровню «средний» или «высокий».

## 10.2 Описание угроз безопасности ПДн

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Класс угроз |  |  | Источник |  |  | Способ реализации | |  |  | Объект |  |  |  | Нарушаемые |  |  | Вероятность |  |  |  |
|  |  |  |  | угроз |  |  |  |  | воздействия | |  |  | свойства ИБ |  |  | реализации |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | Угрозы 1-го типа |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | |  |  |  |  |  |  | | |  |  | |  |  |  |  |  |
|  |  | 1. Угроза НСД | с |  | Внутренний | |  | Доступ в | операционную | среду |  | Технические | | |  | Нарушение | |  | Средняя | |  |  |
|  |  |  | нарушитель | |  | ИСПДн, | реализуемый | при |  | средства | ИСПДн | |  | конфиденциальн | |  | вероятность | |  |  |
|  |  | применением |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | помощи | эксплуатации | НДВ |  | (АРМ |  |  |  | ости, | |  |  |  |  |  |
|  |  | стандартных |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | (уязвимостей системного ПО), | | |  | пользователей, | | |  | целостностии | |  |  |  |  |  |
|  |  | функций |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | осуществляемый | | при |  | сервера |  |  |  | доступности | |  |  |  |  |  |
|  |  | операционной |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | физическом доступе к ИСПДн | | |  | приложений/БД | | |  | ПДн | |  |  |  |  |  |
|  |  | системы |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | или | средствам | ввода |  | ИСПДн) |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | информации в ИСПДн | |  |  | Программные | | |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  | средства | ИСПДн: | |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  | ОС |  |  |  |  |  |  |  |  |  |  |

Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:

1. Используется лицензионное системное ПО надежных производителей.
2. На рабочих станциях пользователей, функционирующих под управлением ОС версии не ниже Windows 7, устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.
3. 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.
4. Идентификация и аутентификация пользователей при входе в ОС на рабочих станциях осуществляется по доменным учетным записям и паролям.
5. Обеспечивается разграничение доступа пользователей к ИСПДн.

Факторы, повышающие вероятность реализации угрозы:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Класс угроз | |  |  |  | Источник | |  |  | Способ реализации | | |  |  | Объект |  |  |  | Нарушаемые | |  |  | Вероятность |  |  |  |
|  |  |  |  |  | угроз |  |  |  |  |  | воздействия | |  |  | свойства ИБ | |  |  | реализации |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 1. | | | Не | осуществляется | | | | настройка | безопасности | | | ОС | на рабочих | | | станциях | |  |  |  |  |  |
|  |  |  |  |  |  |  | пользователей. | | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 2. | | | При покидании пользователем рабочего места не производится блокировка АРМ. | | | | | | | | | | | | | | |  |  |  |  |  |
|  |  |  |  |  | 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, не настроены параметры блокирования рабочей | | | | | | | | | | | | | | | |  |  |  |  |  |
|  |  |  |  |  |  |  | станции после определенного периода неактивности. | | | | | | | | | |  |  |  |  |  |  |  |  |  |  |  |
|  |  | 2. Угроза | НСД с | |  |  | Внутренний | | |  | Реализуется путем эксплуатации | | | |  | Технические | |  |  | Нарушение | | |  | Средняя | |  |  |
|  |  |  |  | нарушитель | | |  | НДВ | в | системном | ПО |  | средства | ИСПДн: | |  | конфиденциальн | | |  | вероятность | |  |  |
|  |  | применением | | |  |  |  |  |  |  |  |  |
|  |  |  |  | Внешний | |  |  | (известных уязвимостей) | | |  |  | сервера |  |  |  | ости, |  |  |  |  |  |  |  |
|  |  | специально | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | нарушитель | | |  |  |  |  |  |  | приложений/БД | | |  | целостностии | | |  |  |  |  |  |
|  |  | созданных | для | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | этого программ | | |  |  |  |  |  |  |  |  |  |  |  | ИСПДн |  |  |  | доступности | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  | Программные | |  |  | ПДн |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | средства | ИСПДн: | |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | ОС |  |  |  |  |  |  |  |  |  |  |  |

Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:

1. Используется лицензионное системное ПО надежных производителей.
2. На рабочих станциях пользователей, функционирующих под управлением ОС версии не ниже Windows 7, устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.
3. На рабочих станциях установлено антивирусное ПО. Осуществляется регулярное обновление антивирусного ПО. Управление антивирусным ПО осуществляется централизовано.
4. Идентификация и аутентификация пользователей при входе в ОС на рабочих станциях осуществляется по доменным учетным записям и паролям.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Класс угроз |  |  | Источник | |  | Способ реализации |  |  | Объект |  |  | Нарушаемые |  |  | Вероятность |  |  |
|  |  |  | угроз |  |  |  |  | воздействия |  |  | свойства ИБ |  |  | реализации |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | 5. | | Обеспечивается разграничение доступа пользователей к ИСПДн. | | | | | | | | | |  |  |  |  |
|  |  |  |  | Факторы, повышающие вероятность реализации угрозы: | | | | | | | |  |  |  |  |  |  |  |
|  |  |  | 1. | | Не осуществляется настройка безопасности ОС на рабочих станциях | | | | | | | | | |  |  |  |  |
|  |  |  |  | пользователей. | | | |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | 2. | | При покидании пользователем рабочего места не производится блокировка АРМ. | | | | | | | | | |  |  |  |  |
|  |  |  | 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, не настроены параметры блокирования рабочей | | | | | | | | | | |  |  |  |  |
|  |  |  |  | станции после определенного периода неактивности. | | | | | | | |  |  |  |  |  |  |  |
|  | 3. Угрозы | типа |  | Внешний | |  | Реализуется путем эксплуатации | |  | Программные | |  | Нарушение | |  | Низкая | |  |
|  |  | нарушитель | |  | уязвимостей НДВ в системном | |  | средства ИСПДн - | |  | доступности | |  | вероятность | |  |
|  | «Отказ | в |  |  |  |  |  |  |
|  | обслуживании», в | |  |  |  |  | ПО |  |  | ОС | |  | ПДн | |  |  |  |  |
|  |  | Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы: | | | | | | | | | | |  |  |  |  |
|  | том | числе |  |  |  |  |  |
|  | 1. | | Используется лицензионное системное ПО надежных производителей. | | | | | | | | | |  |  |  |  |
|  | использование | |  |  |  |  |
|  | 2. | | При осуществлении взаимодействия с сетью Интернет используются средства | | | | | | | | | |  |  |  |  |
|  | известных |  |  |  |  |  |
|  |  |  | межсетевого экранирования. | | | |  |  |  |  |  |  |  |  |  |  |  |
|  | уязвимостей в ПО | |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 3. | | В ЛВС используются только коммутаторы и маршрутизаторы (хабы не | | | | | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | используются). | | | |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | 4. | | На рабочих станциях пользователей, функционирующих под управлением ОС | | | | | | | | | |  |  |  |  |
|  |  |  |  | версии не ниже Windows 7, устанавливаются обновления и патчи для системного ПО, | | | | | | | | | | |  |  |  |  |
|  |  |  |  | сервисов и служб, которые закрывают известные и новые уязвимости. | | | | | | | | | | |  |  |  |  |
|  | 4. Угрозы |  |  | Внешний | |  | Реализуется путем эксплуатации | |  | Программные | |  | Нарушение | |  | Низкая | |  |
|  |  |  | нарушитель | |  | уязвимостей, | вызванных |  | средства ИСПДн: | |  | конфиденциальн | |  | вероятность | |  |
|  | удаленного |  |  |  |  |  |  |  |
|  |  |  |  |  |  | наличием НДВ в системном ПО | |  | ОС | |  | ости, | |  |  |  |  |
|  | запуска |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  | целостностии | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Класс угроз |  |  |  | Источник | |  | Способ реализации |  |  | Объект |  |  | Нарушаемые |  |  | Вероятность |  |  |  |
|  |  |  |  |  | угроз |  |  |  |  | воздействия |  |  | свойства ИБ |  |  | реализации |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | приложений, в том | |  |  |  |  |  |  |  |  |  |  |  | доступности | |  |  |  |  |  |
|  |  | числе: | |  |  |  |  |  |  |  |  |  |  |  | ПДн | |  |  |  |  |  |
|  |  | - распространение | |  |  | Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы: | | | | | | | | | | |  |  |  |  |  |
|  |  | файлов, | | 1. | | | Используется лицензионное системное ПО надежных производителей. | | | | | | | | | |  |  |  |  |  |
|  |  | содержащих | | 2. | | | На рабочих станциях пользователей, функционирующих под управлением ОС | | | | | | | | | |  |  |  |  |  |
|  |  | несанкционирован | |  |  | версии не ниже Windows 7, устанавливаются обновления и патчи для системного ПО, | | | | | | | | | | |  |  |  |  |  |
|  |  | ный исполняемый | |  |  | сервисов и служб, которые закрывают известные и новые уязвимости. | | | | | | | | | | |  |  |  |  |  |
|  |  | код; | | 3. | | | На рабочих станциях установлено антивирусное ПО. Осуществляется регулярное | | | | | | | | | |  |  |  |  |  |

* переполнение обновление антивирусного ПО. Управление антивирусным ПО осуществляется

буферацентрализовано.

приложений-4.При осуществлении взаимодействия с сетью Интернет используются средства

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | серверов; | межсетевого экранирования. | | | |  |  |  |  |  |  |  |
|  |  | -использование | 5. | Обеспечивается разграничение доступа пользователей к ИСПДн. | | | | | | |  |  |  |
|  |  | возможностей |  |  |  |  |  |  |  |  |  |  |  |
|  |  | удаленного |  |  |  |  |  |  |  |  |  |  |  |
|  |  | управления |  |  |  |  |  |  |  |  |  |  |  |
|  |  | системой |  |  |  |  |  |  |  |  |  |  |  |
|  |  | Угрозы 2-го типа |  |  |  |  |  |  |  |  |  |  |  |
|  |  | 5. Угроза НСД с | Внутренний | | Доступ в | операционную | среду | Технические | | Нарушение | Средняя |  |  |
|  |  | нарушитель | | ИСПДн, | реализуемый | при | средства | ИСПДн | конфиденциальн | вероятность |  |  |
|  |  | применением |  |  |
|  |  |  |  | помощи | эксплуатации | НДВ | (АРМ |  | ости, |  |  |  |
|  |  | стандартных |  |  |  |  |  |  |
|  |  |  |  | (уязвимостей прикладного ПО), | | | пользователей, | | целостностии |  |  |  |
|  |  | функций |  |  |  |  |  |
|  |  |  |  | осуществляемый | | при | сервера |  | доступности |  |  |  |
|  |  | прикладного ПО |  |  |  |  |  |  |
|  |  |  |  | физическом доступе к ИСПДн | | | приложений/БД | | ПДн |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  | или | средствам | ввода | ИСПДн) |  |  |  |  |  |
|  |  |  |  |  | информации в ИСПДн | |  | Программные | |  |  |  |  |
|  |  |  |  |  |  |  |  | средства | ИСПДн: |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Класс угроз |  |  |  | Источник |  |  |  | Способ реализации |  |  | Объект |  |  |  | Нарушаемые |  | Вероятность |  |  |
|  |  |  |  | угроз |  |  |  |  |  | воздействия |  |  |  | свойства ИБ |  | реализации |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

ППО, СУБД

Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:

1. Используется лицензионное ПО надежных производителей.
2. На рабочих станциях пользователей устанавливаются обновления и патчи для прикладного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.
3. 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.
4. Идентификация и аутентификация пользователей при входе в ОС на рабочих станциях осуществляется по доменным учетным записям и паролям.
5. Обеспечивается разграничение доступа пользователей к ИСПДн.

Факторы, повышающие вероятность реализации угрозы:

1. Доступ к USB портам, устройствам чтения/записи оптических дисков, дисководам на рабочих станциях работников Института не ограничен.
2. При покидании пользователем рабочего места не производится блокировка АРМ.
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.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 6. Угроза | НСД с | Внутренний | Реализуется путем эксплуатации | Технические | Нарушение | Средняя |  |
| нарушитель | НДВвприкладномПО | средства ИСПДн: | конфиденциальн | вероятность |  |
| применением | |  |
| Внешний | (известных уязвимостей) | сервера | ости, |  |  |
| специально | |  |  |
| нарушитель |  | приложений/БД | целостностии |  |  |
| созданных | для |  |  |  |
|  |  |  |  | ИСПДн | доступности |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Класс угроз |  |  |  | Источник |  |  | Способ реализации |  |  | Объект |  |  | Нарушаемые |  |  | Вероятность |  |  |  |
|  |  |  |  |  | угроз |  |  |  |  | воздействия |  |  | свойства ИБ |  |  | реализации |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | этого программ | |  |  |  |  |  |  |  |  | Программные | |  | ПДн | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  | средства ИСПДн: | |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  | ППО, СУБД | |  |  |  |  |  |  |  |  |

Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:

1. Используется лицензионное ПО надежных производителей.
2. На рабочих станциях пользователей устанавливаются обновления и патчи для прикладного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.
3. На рабочих станциях установлено антивирусное ПО. Осуществляется регулярное обновление антивирусного ПО. Управление антивирусным ПО осуществляется централизовано.
4. Идентификация и аутентификация пользователей при входе в ОС на рабочих станциях осуществляется по доменным учетным записям и паролям.
5. Обеспечивается разграничение доступа пользователей к ИСПДн.

Факторы, повышающие вероятность реализации угрозы:

1. Доступ к USB портам, устройствам чтения/записи оптических дисков, дисководам на рабочих станциях работников Института не ограничен.
2. При покидании пользователем рабочего места не производится блокировка АРМ.
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.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 7. Угрозы | типа | Внешний | Реализуется путем эксплуатации | Программные | Нарушение | Низкая |  |
| нарушитель | уязвимостей НДВ в прикладном | средства ИСПДн | доступности | вероятность |  |
| «Отказ | в |  |
| обслуживании», в | |  | ПО | ППО, СУБД | ПДн |  |  |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы: | | | |  |  |
| том | числе |  |  |
|  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Класс угроз | |  |  | Источник | |  | Способ реализации |  |  | Объект |  |  | Нарушаемые |  |  | Вероятность |  |  |
|  |  |  | угроз |  |  |  |  | воздействия |  |  | свойства ИБ |  |  | реализации |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | использование | | | 1. | | Используется лицензионное ПО надежных производителей. | | | | | | |  |  |  |  |  |  |  |
|  | известных | | | 2. | | При осуществлении взаимодействия с сетью Интернет используются средства | | | | | | | | | |  |  |  |  |
|  | уязвимостей в ПО | | |  | межсетевого экранирования. | | | |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | 3. | | В ЛВС используются только коммутаторы и маршрутизаторы (хабы не | | | | | | | | | |  |  |  |  |
|  |  |  |  |  | используются). | | | |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | 4. | | На рабочих станциях пользователей, функционирующих под управлением ОС | | | | | | | | | |  |  |  |  |
|  |  |  |  |  | версии не ниже Windows 7, 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 | | |  | Внешний | |  | Реализуется путем эксплуатации | |  | Программные | |  | Нарушение | |  | Низкая | |  |
|  |  | нарушитель | |  | уязвимостей, | вызванных |  | средства ИСПДн: | |  | конфиденциальн | |  | вероятность | |  |
|  | удаленного | | |  |  |  |  |  |  |
|  |  |  |  |  | наличием НДВ в | прикладном |  | ППО, СУБД | |  | ости, | |  |  |  |  |
|  | запуска | | |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | ПО |  |  |  |  |  | целостностии | |  |  |  |  |
|  | приложений, в том | | |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  | доступности | |  |  |  |  |
|  | числе: | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  | ПДн | |  |  |  |  |
|  | - распространение | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы: | | | | | | | | | | |  |  |  |  |
|  | файлов, | | | 1. | | Используется лицензионное системное ПО надежных производителей. | | | | | | | | | |  |  |  |  |
|  | содержащих | | |  |  |  |  |
|  | 2. | | На рабочих станциях пользователей, функционирующих под управлением ОС | | | | | | | | | |  |  |  |  |
|  | несанкционирован | | |  |  |  |  |
|  |  | версии не ниже Windows 7, устанавливаются обновления и патчи для системного ПО, | | | | | | | | | | |  |  |  |  |
|  | ный | исполняемый | |  |  |  |  |  |
|  |  | сервисов и служб, которые закрывают известные и новые уязвимости. | | | | | | | | | | |  |  |  |  |
|  | код; |  |  |  |  |  |  |  |
|  |  |  | 3. | | На рабочих станциях установлено антивирусное ПО. Осуществляется регулярное | | | | | | | | | |  |  |  |  |
| - | | переполнение | |  |  |  |  |
|  | буфера | | |  | обновление антивирусного ПО. Управление антивирусным ПО осуществляется | | | | | | | | | | |  |  |  |  |
|  |  | централизовано. | | | |  |  |  |  |  |  |  |  |  |  |  |
|  | приложений- | | |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 4. | | При осуществлении взаимодействия с сетью Интернет используются средства | | | | | | | | | |  |  |  |  |
|  | серверов; | | |  |  |  |  |
|  |  | межсетевого экранирования. | | | |  |  |  |  |  |  |  |  |  |  |  |
| - | | использование | |  |  |  |  |  |  |  |  |  |  |  |  |
| 5. | | Обеспечивается разграничение доступа пользователей к ИСПДн. | | | | | | | | | |  |  |  |  |
|  | возможностей | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Класс угроз | |  |  | Источник |  |  | Способ реализации | | | |  |  |  |  | Объект |  |  |  | Нарушаемые |  |  | Вероятность |  |  |
|  |  |  | угроз |  |  |  |  |  |  | воздействия | |  |  | свойства ИБ |  |  | реализации |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | удаленного | | |  | Факторы, | повышающие | | | | вероятность | | | | реализации | | | угрозы: средства анализа | | | | |  |  |  |  |
|  | управления | | |  | защищенности не используются. | | | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | системой |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Угрозы 3-го типа | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 9. Угрозы | утечки | |  | Внешний |  |  | Перехват |  |  | акустической | | | |  | Технические | | |  | Нарушение | |  | Маловероятн | |  |
|  |  | нарушитель |  |  | (речевой) |  | информации | | | | с |  | средства обработки | | |  | конфиденциальн | |  | ая | |  |
|  | акустической | | |  |  |  |  |  |  |  |  |
|  |  |  |  |  | использованием | | | аппаратуры, | | | |  | ПДн, | ВТСС, | |  | ости ПДн | |  | вероятность | |  |
|  | (речевой) |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | регистрирующей акустические и | | | | | | |  | строительные | | |  |  |  |  |  |  |  |
|  | информации | | |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | виброакустические | | |  | волны, | | а |  | конструкции, | | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | также |  | электромагнитные | | | | |  | инженерно- | | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | излучения, | | оптические | | | | и |  | технические | | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | электрические | | |  | сигналы, | | |  | коммуникации, | | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | модулированные | | |  |  |  |  |  | персонал ИСПДн | | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | информативным | | | акустическим | | | |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | сигналом. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | Перехват |  |  | акустической | | | |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | (речевой) |  | информации | | | | с |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | использованием | | | специальных | | | |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | электронных | | устройств | | | съема | |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | речевой информации | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы: | | | | | | | | | | | | | | | | |  |  |  |  |
|  |  |  |  |  | речевой (акустический) ввод/вывод персональных данных в данной ИСПДн не | | | | | | | | | | | | | | | | |  |  |  |  |
|  |  |  |  |  | предусмотрен. | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 10. Угрозы | | |  | Внешний |  |  | Просмотр | ПДн | | с | помощью | | |  | Технические | | |  | Нарушение | |  | Низкая | |  |
|  |  | нарушитель |  |  | оптических | |  |  |  |  |  |  | средства обработки | | |  | конфиденциальн | |  | вероятность | |  |
|  | утечки | видовой | |  |  |  |  |  | средств с | | |  |  |  |  |
|  | информации | | |  | Внутренний |  |  | (оптикоэлектронных) | | | |  | ПДн, | помещения, | |  | ости ПДн | |  |  |  |  |
|  |  | нарушитель |  |  | экранов | дисплеев | | | и | других | |  | персонал ИСПДн | | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Класс угроз |  |  |  | Источник |  |  |  | Способ реализации |  |  | Объект |  |  |  | Нарушаемые |  | Вероятность |  |  |
|  |  |  |  | угроз |  |  |  |  |  | воздействия |  |  |  | свойства ИБ |  | реализации |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

средств отображения средств

вычислительной техники,

информационно-

вычислительных комплексов,

технических средств обработки

графической, видео и буквенно-

цифровой информации

Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:

1. 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.
2. Средства отображения информации в офисных помещениях защищены от визуального просмотра.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Внешний | Просмотр ПДн | | с помощью | | Технические | Нарушение | Низкая |
| нарушитель | специальных |  | электронных | | средства обработки | конфиденциальн | вероятность |
|  | устройств съема, внедренных в | | | | ПДн, помещения, | ости ПДн |  |
|  | служебных | помещениях | | или | персонал ИСПДн |  |  |
|  | скрытно |  | используемых | |  |  |  |
|  | физическими | лицами | | при |  |  |  |
|  | посещении | ими | служебных | |  |  |  |
|  | помещений |  |  |  |  |  |  |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы: | | | | | | |  |
| 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. | | | |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Класс угроз | |  |  | Источник |  |  | Способ реализации | |  |  |  | Объект |  |  |  |  | Нарушаемые |  |  | Вероятность |  |  |
|  |  |  | угроз |  |  |  |  |  | воздействия | |  |  |  | свойства ИБ |  |  | реализации |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 11. | | Угрозы |  |  | Внешний | |  | Перехват | техническими | | |  | Инженерно- | |  |  |  | Нарушение | |  | Низкая | |  |
|  |  | нарушитель | |  | средствами | побочных | | (не |  | технические | |  |  |  | конфиденциальн | |  | вероятность | |  |
|  | утечки | |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | связанных | с | прямым | |  | коммуникации | |  |  |  | ости ПДн | |  |  |  |  |
|  | информации | | по |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | | |  | функциональным | | значением | |  | (цепи |  |  |  |  |  |  |  |  |  |  |
|  | каналам ПЭМИН | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | | |  | элементов |  | ИСПДн) | |  | электропитания, | |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | информативных | |  |  |  | шины заземления и | | | |  | | |  |  |  |  |
|  |  |  |  |  |  |  |  | электромагнитных | | полей | и |  | т.д.) Института | |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | электрических |  | сигналов, | |  | ВТСС (средства | | и | |  | | |  |  |  |  |
|  |  |  |  |  |  |  |  | возникающих | при | обработке | |  | системы | охранной | | |  | | |  |  |  |  |
|  |  |  |  |  |  |  |  | ПДн техническими | | средствами | |  | и | пожарной | | |  | | |  |  |  |  |
|  |  |  |  |  |  |  |  | ИСПДн |  |  |  |  | сигнализации | | и | |  | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  | т.д.) Института | |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  | Линии | связи | и | |  | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  | передачи данных | |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  | Технические | |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  | средства обработки | | | |  | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  | ПДн | (рабочие | | |  | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  | станции, | сервера и | | |  | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  | т.д.) |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы: | | | | | | | | | | | | | | |  |  |  |  |
|  |  |  |  |  | при обработке информации на АРМ пользователей, 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 |  |  | Внутренний | |  | Реализуются с | использованием | | |  | Программные | |  |  |  | Нарушение | |  | Средняя | |  |
|  |  | нарушитель | |  | отчуждаемых |  | носителей | |  | средства | ИСПДн: | | | конфиденциальн | | |  | вероятность | |  |
|  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Класс угроз | | |  |  | Источник |  |  | Способ реализации | | | |  |  |  |  |  | Объект |  |  |  | Нарушаемые |  |  | Вероятность |  |  |
|  |  |  | угроз |  |  |  |  |  |  |  | воздействия | |  |  | свойства ИБ |  |  | реализации |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | модификации | | | |  | Внешний | |  | информации. | | Осуществляются | | | | | |  | базовая | система | |  | ости, |  |  |  |  |  |
|  | базовой | | системы | |  | нарушитель | |  | перехват |  | паролей | | |  |  | или |  | ввода-вывода | | |  | целостности | и |  | | |  |
|  | ввода/вывода | | | |  |  |  |  | идентификаторов, | | | модификация | | | | |  | (BIOS). |  |  |  | доступности |  |  |  |  |  |
|  | (BIOS), перехвата | | | |  |  |  |  | программного | |  | обеспечения | | | | |  | Технические | | |  | ПДн |  |  |  |  |  |
|  | управления | | | |  |  |  |  | базовой системы ввода-вывода | | | | | | | |  | средства ИСПДн | | |  |  |  |  |  |  |  |
|  | загрузкой, | |  |  |  |  |  |  | (BIOS), | перехват | | | управления | | | |  |  |  |  |  |  |  |  |  |  |  |
|  | перехвата | | или | |  |  |  |  | загрузкой | с | целью | | изменения | | | |  |  |  |  |  |  |  |  |  |  |  |
|  | подбора | | паролей | |  |  |  |  | необходимой | | технологической | | | | | |  |  |  |  |  |  |  |  |  |  |  |
|  | или |  |  |  |  |  |  |  | информации | | для | | получения | | | |  |  |  |  |  |  |  |  |  |  |  |
|  | идентификаторов, | | | |  |  |  |  | НСД в | операционную | | | | |  | среду |  |  |  |  |  |  |  |  |  |  |  |
|  | а |  | также | |  |  |  |  | ИСПДн |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | использование | | | |  | Применяемые защитные меры, | | | | | | снижающие вероятность угроз: доступ в помещения | | | | | | | | | | | |  | | |  |
|  | технологических | | | |  | Института, | | где расположены рабочие станции пользователей, ограничен | | | | | | | | | | | | | | | и |  | | |  |
|  | паролей BIOS | | | |  | контролируется. В случае удаленного использования рабочих станций за границами | | | | | | | | | | | | | | | | | |  | | |  |
|  |  |  |  |  |  | контролируемой зоны Института, ответственность за безопасность рабочих станций | | | | | | | | | | | | | | | | | |  | | |  |
|  |  |  |  |  |  | возложена на работников. | | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | Факторы,повышающиевероятностьреализацииугрозы:аутентификация | | | | | | | | | | | | | | | | | |  | | |  |
|  |  |  |  |  |  | пользователей при доступе к BIOS не осуществляется. | | | | | | | | | | | | |  |  |  |  |  |  |  |  |  |
| 13. | | Угроза НСД | | |  | Внутренний | |  | Доступ в | операционную | | | | | | среду |  | Программные | | |  | Нарушение |  |  | Высокая | |  |
|  | нарушитель | |  | ИСПДн | с | использованием | | | | | |  | средства | ИСПДн: | |  | конфиденциальн | | вероятность | | |  |
|  | с | применением | | |  |  |  |  |  |
|  | стандартных | | | |  | Внешний | |  | программных | | и | программно- | | | | |  | ОС, | СУБД, | |  | ости, |  |  |  |  |  |
|  |  | нарушитель | |  | аппаратных | |  |  |  |  | средств | |  | прикладные | | |  | целостности | и |  |  |  |  |
|  | функций | |  |  |  |  |  |  |  |  |  |  |  | | |  |
|  |  |  |  |  |  |  | ввода/вывода | | рабочих | | | станций | | |  | системы. |  |  |  | доступности |  |  |  |  |  |
|  | операционной | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | (серверов), входящих | | | | | в | состав | |  | Технические | | |  | ПДн |  |  |  |  |  |
|  | системы, | | СУБД, | |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | ИСПДн, | осуществляемый | | | | | | при |  | средства ИСПДн | | |  |  |  |  |  |  |  |
|  | прикладной | | | |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | физическом доступе | | | | к |  | ИСПДн | |  |  |  |  |  |  |  |  |  |  |  |
|  | программы | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | или | средствам | | |  |  |  | ввода |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Класс угроз |  |  |  | Источник |  |  |  | Способ реализации |  |  | Объект |  |  |  | Нарушаемые |  | Вероятность |  |  |
|  |  |  |  | угроз |  |  |  |  |  | воздействия |  |  |  | свойства ИБ |  | реализации |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

информации в ИСПДн

Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:

1. Используется лицензионное ПО надежных производителей.
2. На рабочих станциях пользователей устанавливаются обновления и патчи для прикладного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.
3. 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.
4. Идентификация и аутентификация пользователей при входе в ОС на рабочих станциях осуществляется по доменным учетным записям и паролям.
5. Пароли в открытом виде в ИСПДн не хранятся.
6. Обеспечивается разграничение доступа пользователей к ИСПДн.

Факторы, повышающие вероятность реализации угрозы:

1. Доступ к USB портам, устройствам чтения/записи оптических дисков, дисководам на рабочих станциях работников Института не ограничен.
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.
4. При покидании пользователем рабочего места не производится блокировка АРМ.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 14. Угроза НСД | Внутренний | Реализуется путем эксплуатации | Технические | Нарушение | Высокая |  |
| нарушитель | вредоносного кода с целью | средства ИСПДн: | конфиденциальн | вероятность |  |
|  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Класс угроз | |  |  |  | Источник |  |  | Способ реализации | |  |  | Объект |  |  | Нарушаемые |  |  | Вероятность |  |  |  |
|  |  |  |  |  | угроз |  |  |  |  | воздействия |  |  | свойства ИБ |  |  | реализации |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | с | применением | |  |  | Внешний | |  | получения | доступа | к |  | сервера | |  | ости, |  |  |  |  |  |  |
|  |  | специально | |  |  |  | нарушитель | |  | программным | средствам | |  | приложений/БД | |  | целостности | и | | | |  |  |
|  |  | созданных | | для |  |  |  |  |  | ИСПДн |  |  |  | ИСПДн | |  | доступности |  |  |  |  |  |  |
|  |  | этого программ | |  |  |  |  |  |  |  |  |  |  | Программные | |  | ПДн |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  | средства ИСПДн: | |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  | ППО, СУБД | |  |  |  |  |  |  |  |  |

Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:

1. Используется лицензионное ПО надежных производителей.
2. На рабочих станциях пользователей устанавливаются обновления и патчи для прикладного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.
3. На рабочих станциях установлено антивирусное ПО. Осуществляется регулярное обновление антивирусного ПО. Управление антивирусным ПО осуществляется централизовано.
4. Идентификация и аутентификация пользователей при входе в ОС на рабочих станциях осуществляется по доменным учетным записям и паролям.

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Класс угроз |  |  |  | Источник |  |  | Способ реализации |  |  | Объект |  |  | Нарушаемые |  | Вероятность |  |  |  |
|  |  |  |  |  | угроз |  |  |  |  | воздействия |  |  | свойства ИБ |  | реализации |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

станциях.

1. При покидании пользователем рабочего места не производится блокировка АРМ.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 15. Угроза | |  | Внутренний | | Копирование выгруженной | | из |  | Программные | |  | Нарушение | Высокая |  |
|  | нарушитель | | ИСПДн | информации | на |  | средства | ИСПДн: |  | конфиденциальн | вероятность |  |
| утечки |  |  |  |  |  |
|  |  | Внешний | | отчуждаемые носители | |  |  | ОС, | СУБД, |  | ости ПДн |  |  |
| информации путем | | |  |  |  |  |  |
| нарушитель | |  |  |  |  | прикладные | |  |  |  |  |
| преднамеренного | | |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | системы. |  |  |  |  |  |
| копирования | |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы: | | | | | | | | | |  |  |
| доступных ПДн на | | |  |  |
| 1. | Доступ | в помещения Института, | |  | где расположены | | | рабочие станции | |  |  |
| неучтенные (в том | | |  |  |  |
| числе |  |  | пользователей, ограничен и контролируется. В случае удаленного использования | | | | | | | | | |  |  |
|  |  | рабочих станций за границами контролируемой зоны Института ответственность за | | | | | | | | | |  |  |
| отчуждаемые) | | |  |  |
| безопасность рабочих станций возложена на работников. | | | | | | |  |  |  |  |  |
| носители, а | | также |  |  |  |  |  |
| 2. | Обеспечивается разграничение доступа пользователей к ИСПДн. | | | | | | | | |  |  |
| печать неучтенных | | |  |  |
| копий | документов | | 3. | Идентификация и аутентификация пользователей при входе в ОС на рабочих | | | | | | | | |  |  |
| с | ПДн | на | станциях осуществляется по доменным учетным записям и паролям. | | | | | | | | | |  |  |
| Факторы, повышающие вероятность реализации угрозы: | | | | | | |  |  |  |  |  |
| принтерах | |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |

1. Не осуществляется контроль портов ввода/вывода на АРМ пользователей.
2. Пользователи обладают правами локальных администраторов на своих рабочих станциях.
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. При покидании пользователем рабочего места не производится блокировка АРМ.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 16. Угроза | Внутренний | Доступ в | операционную среду | | Программные | Нарушение | Высокая |  |
| нарушитель | ИСПДн | с | использованием | средства ИСПДн: | конфиденциальн | вероятность |  |
|  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Класс угроз | | |  |  | Источник | |  | Способ реализации |  |  |  | Объект |  |  |  | Нарушаемые | |  |  | Вероятность |  |  |
|  |  |  | угроз |  |  |  |  |  | воздействия | |  |  | свойства ИБ | |  |  | реализации |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | внедрения | |  |  |  | Внешний | |  | вредоносных | программ, |  |  | ОС, | СУБД, | |  | ости, |  |  |  |  |  |  |
|  | вредоносных | | |  |  | нарушитель | |  | загруженных с использованием | |  |  | прикладные | | |  | целостностии | | |  |  |  |  |
|  | программ | |  | с |  |  |  |  | съемных носителей |  |  |  | системы, |  |  |  | доступности | | |  |  |  |  |
|  | использованием | | | |  |  |  |  |  |  |  |  | технические | | |  | ПДн |  |  |  |  |  |  |
|  | съемных | |  |  |  |  |  |  |  |  |  |  | средства ИСПДн. | | |  |  |  |  |  |  |  |  |
|  | носителей, | | а также | |  | Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы: | | | | | | | | | | | | | |  |  |  |  |
|  | в | связи | | с | 1. | | Доступ в помещения Института, | | | | где расположены | | | | | рабочие | | станции | |  |  |  |  |
|  | подключением | | |  |  | пользователей, ограничен и контролируется. В случае удаленного использования | | | | | | | | | | | | | |  |  |  |  |
|  | стороннего | |  |  |  | рабочих станций за границами контролируемой зоны Института ответственность за | | | | | | | | | | | | | |  |  |  |  |
|  | оборудования | | |  |  | безопасность рабочих станций возложена на работников. | | | | | | | |  |  |  |  |  |  |  |  |  |  |
|  | (компьютеров, | | |  | 2. | | Обеспечивается разграничение доступа пользователей к ИСПДн. | | | | | | | | | | |  |  |  |  |  |  |
|  | КПК, | смартфонов, | | | 3. | | Идентификация и аутентификация пользователей при входе в ОС на рабочих | | | | | | | | | | | | |  |  |  |  |
|  | телефонов, | |  |  |  | станциях осуществляется по доменным учетным записям и паролям. | | | | | | | | | | | |  |  |  |  |  |  |
|  | фотоаппаратов, | | |  | 4. | | На рабочих станциях установлено антивирусное ПО. Осуществляется регулярное | | | | | | | | | | | | |  |  |  |  |
|  | видеокамер, флэш- | | | | обновление антивирусного ПО. Управление антивирусным ПО осуществляется | | | | | | | | | | | | | | |  |  |  |  |
|  | дисков и иных | | | | централизовано. | | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | устройств, | | в | том |  | Факторы, повышающие вероятность реализации угрозы: | | | | | | | |  |  |  |  |  |  |  |  |  |  |
|  | числе | имеющих | | | 1. | | Не осуществляется контроль портов ввода/вывода на АРМ пользователей. | | | | | | | | | | | | |  |  |  |  |
|  | выход | |  | в | 2. | | Пользователи обладают правами локальных администраторов на своих рабочих | | | | | | | | | | | | |  |  |  |  |
|  | беспроводные сети | | | |  | станциях. | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | связи) | |  |  | 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. | | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 17. | | Угроза | |  |  | Внутренний | |  | Использование | программ- |  |  | Технические | | |  | Нарушение | | |  | Высокая | |  |
|  |  | нарушитель | |  | анализаторов | пакетов |  |  | средства | ИСПДн | |  | конфиденциальн | | |  | вероятность | |  |
|  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Класс угроз |  |  |  | Источник |  |  | Способ реализации | |  |  | Объект |  |  | Нарушаемые | |  |  | Вероятность |  |  |  |
|  |  |  |  |  | угроз |  |  |  |  | воздействия |  |  | свойства ИБ | |  |  | реализации |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | «Анализа сетевого | |  |  | Внешний | |  | (снифферов) для перехвата ПДн | | |  | (каналы связи) | |  | ости: |  |  |  |  |  |  |  |
|  |  | трафика» | |  |  | нарушитель | |  | (ииной | конфиденциальной | |  |  |  |  | исследование | |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | информации), а также для | | |  |  |  |  | характеристик | | | | | |  |  |
|  |  |  |  |  |  |  |  |  | перехвата | идентификаторов и | |  |  |  |  | сетевого |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | паролей удаленного доступа (к | | |  |  |  |  | трафика, |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | сетевым службам) | | |  |  |  |  | перехват |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | передаваемых | | | | | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | данных, | в | том | | | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | числе |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | идентификаторо | | | | | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | ви | паролей | | | | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | пользователей | | |  | | |  |  |

Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:

1. 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.
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 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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Класс угроз |  |  | Источник | |  | Способ реализации | | | |  |  |  | Объект |  |  |  | Нарушаемые | |  |  | Вероятность |  |  |
|  |  |  | угроз |  |  |  |  |  | воздействия | |  |  | свойства ИБ | |  |  | реализации |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | 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. | | | | | | | | |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | 2. | | Пользователи обладают правами локальных администраторов на своих рабочих | | | | | | | | | | | | | | | |  |  |  |  |
|  |  |  |  | станциях. | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | 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. | | | | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 18. Угроза | |  | Внутренний | |  | Передача | | запросов | | сетевым | |  | Технические | | |  | Нарушение | | |  | Высокая | |  |
|  |  | нарушитель | |  | службам | | хостов ИСПДн | | | и |  | средства | ИСПДн | |  | конфиденциальн | | |  | вероятность | |  |
|  | сканирования сети | |  |  |  |  |  |  |
|  |  | Внешний | |  | анализ ответов на них с целью: | | | | |  |  | (каналы | связи), | |  | ости: | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | нарушитель | | - | | инвентаризации | | | сетевых | |  | программные | | |  | определение | | |  |  |  |  |
|  |  |  |  |  |  |  | ресурсов (поиск узлов сети, | | | | | |  | средства ИСПДн | | |  | протоколов, | | |  |  |  |  |
|  |  |  |  |  |  |  | определение их адресов, типов | | | | | |  |  |  |  |  | доступных | | |  |  |  |  |
|  |  |  |  |  |  |  | ОС); | |  |  |  |  |  |  |  |  |  | портов сетевых | | |  |  |  |  |
|  |  |  |  |  |  | - | | выявления активных | | | сетевых | |  |  |  |  |  | служб, | | |  |  |  |  |
|  |  |  |  |  |  |  | служб, используемых портов, | | | | | |  |  |  |  |  | идентификаторо | | |  |  |  |  |
|  |  |  |  |  |  |  | версий программ (уязвимых); | | | | |  |  |  |  |  |  | в | соединений, | |  |  |  |  |
|  |  |  |  |  |  |  | - выявления неиспользуемых, но | | | | | |  |  |  |  |  | активных | | |  |  |  |  |
|  |  |  |  |  |  |  | установленных | | | сетевых служб | | |  |  |  |  |  | сетевых | | |  |  |  |  |
|  |  |  |  |  |  |  | (уязвимых) | |  |  |  |  |  |  |  |  |  | сервисов, | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | идентификаторо | | |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Класс угроз |  |  |  | Источник |  |  |  | Способ реализации |  |  | Объект |  |  |  | Нарушаемые |  | Вероятность |  |  |
|  |  |  |  | угроз |  |  |  |  |  | воздействия |  |  |  | свойства ИБ |  | реализации |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

в и паролей

пользователей.

Нарушение

доступности:

возможен отказ в

обслуживании

сканируемых

сетевых

сервисов

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. При осуществлении взаимодействия с сетью Интернет используются средства межсетевого экранирования.
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. Пользователи обладают правами локальных администраторов на своих рабочих станциях.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Класс угроз |  |  |  | Источник |  |  | Способ реализации | |  |  |  | Объект |  |  |  | Нарушаемые |  |  | Вероятность |  |  |  |
|  |  |  |  |  | угроз |  |  |  |  |  | воздействия | |  |  | свойства ИБ |  |  | реализации |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | 19. Угроза | |  |  | Внутренний | |  | Перебор паролей (в том числе с | | | |  | Технические | | |  | Нарушение |  |  | Высокая | |  |  |
|  |  |  |  | нарушитель | |  | использованием | |  |  |  | средства | ИСПДн | |  | конфиденциальн вероятность | | | | |  |  |
|  |  | выявления паролей | |  |  |  |  |  |  |  |  |  |
|  |  |  |  | Внешний | |  | специализированного | | | ПО), |  | (каналы | связи), | |  | ости, |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | нарушитель | |  | установка |  | вредоносных | |  | программные | | |  | целостности | и | | | |  |  |
|  |  |  |  |  |  |  |  |  | программ | для | перехвата | |  | средства ИСПДн | | |  | доступности |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | паролей, | подмена | доверенного | |  |  |  |  |  | ПДн: |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | объекта | сети | (IP-spoofing), | |  |  |  |  |  | выполнение |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | перехват | пакетов | | (sniffing). |  |  |  |  |  | любого |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | Взлом перехваченных | | | в сети |  |  |  |  |  | действия, |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | защищенных паролей (хэш) | | | |  |  |  |  |  | связанного | с | | | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | получением |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | несанкциониров | | | | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | анного доступа |  |  |  |  |  |  |

Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:

1. На рабочих станциях 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 пользователей при входе в ОС по доменным учетным записям и паролям.
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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Класс угроз |  |  | Источник | |  | Способ реализации | | | |  |  | Объект |  |  | Нарушаемые |  |  | Вероятность |  |  |
|  |  |  | угроз |  |  |  |  | воздействия |  |  | свойства ИБ |  |  | реализации |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | 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. | | 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 | |  | Внутренний | |  | Несанкционированное | | | |  |  | Технические | |  | Нарушение | |  | Средняя | |  |
|  |  | нарушитель | |  | использование | |  | протоколов | | средства ИСПДн | | |  | конфиденциальн | |  | вероятность | |  |
|  | навязывания | |  |  |  |  |  |  |
|  |  | Внешний | |  | маршрутизации | | | (RIP, | OSPF, |  |  |  |  | ости, | |  |  |  |  |
|  | ложного маршрута | |  |  |  | | |  |  |  |  |  |
|  |  | нарушитель | |  | LSP, | EIGRP) | и | управления | |  |  |  |  | целостностии | |  |  |  |  |
|  | сети | |  |  |  | | |  |  |  |  |  |
|  |  |  |  |  | сетью | (ICMP, | | SNMP) | для |  |  |  |  | доступности: | |  |  |  |  |
|  |  |  |  |  |  |  |  | | |  |  |  |  |  |
|  |  |  |  |  |  |  | внесения | | изменений | | в |  | | |  | несанкциониров | |  |  |  |  |
|  |  |  |  |  |  |  | маршрутно-адресные таблицы | | | | |  | | |  | анное изменение | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | маршрутно- | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | адресных | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | данных, анализ и | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | модификация | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | передаваемых | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | данных, | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | навязывание | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | ложных | |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Класс угроз |  |  |  | Источник |  |  | Способ реализации |  |  | Объект |  |  | Нарушаемые |  |  | Вероятность |  |  |  |
|  |  |  |  |  | угроз |  |  |  |  | воздействия |  |  | свойства ИБ |  |  | реализации |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | сообщений | |  |  |  |  |  |

Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:

1. Обеспечивается разграничение доступа к кроссовому оборудованию.
   1. 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.
   2. В ЛВС используются только коммутаторы и маршрутизаторы (хабы не используются).
   3. 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.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 21. Угроза | Внутренний | Перехват поискового запроса в | Технические | Нарушение | Средняя |  |
| нарушитель | протоколах удаленного поиска | средства ИСПДн | конфиденциальн | вероятность |  |
| внедрения ложного |  |
| объекта сети | Внешний | (ARP, DNS, WINS) - в сетях со |  | ости, |  |  |
| нарушитель | стеком протоколов TCP/IP, и |  | целостностии |  |  |
|  |  |  |  |
|  |  | выдача на него ложного ответа, |  | доступности |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Класс угроз |  |  |  | Источник |  |  | Способ реализации | |  |  | Объект |  |  | Нарушаемые |  |  | Вероятность |  |  |  |
|  |  |  |  |  | угроз |  |  |  |  | воздействия |  |  | свойства ИБ |  |  | реализации |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | использование | | которого |  | | |  | ПДн: перехват и | | | | |  |  |
|  |  |  |  |  |  |  |  |  | приводит | к | требуемому |  | | |  | просмотр |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | изменению | в | маршрутно- |  | | |  | трафика, |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | адресных данных | |  |  |  |  |  | несанкциониров | | | | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | анный доступ | к | | | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | сетевым |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | ресурсам, |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | навязывание |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | ложной |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | информации |  |  |  |  |  |  |

Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:

1. 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.
   1. Обеспечивается разграничение доступа к кроссовому оборудованию.
   2. В ЛВС используются только коммутаторы и маршрутизаторы (хабы не используются).
   3. 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.
   1. Излишнее ПО, не являющееся необходимым для реализации бизнес-процессов, не удалено с рабочих станций пользователей.
   2. Для аутентификации используются слабые пароли, настройки парольной

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Класс угроз | |  |  | Источник |  |  | Способ реализации | | | |  |  |  |  | Объект |  |  |  | Нарушаемые | | |  |  | Вероятность |  |  |
|  |  |  | угроз |  |  |  |  |  |  | воздействия | |  |  | свойства ИБ | | |  |  | реализации |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 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 | |  | Внутренний | | - | | привлечение | | части | | ресурсов | |  | Технические | | |  | Нарушение | | |  |  | Средняя | |  |
|  | нарушитель | |  | ИСПДн на обработку | | | | | пакетов, | |  | средства | ИСПДн | |  | доступности | | | за | вероятность | | |  |
|  | «Отказ | | в |  |  |  |  |  |
|  | обслуживании», в | | |  | Внешний | |  | передаваемых | | |  |  |  |  |  | (каналы | связи), | |  | счет: |  |  |  |  |  |  |  |
|  |  | нарушитель | |  | злоумышленником | | | |  |  | со |  | программные | | | - | | снижения | | |  |  |  |  |
|  | том числе: | |  |  |  |  |  |  |  | | |  |
|  |  |  |  |  |  | снижением | | |  | пропускной | | |  | средства ИСПДн | | |  | пропускной | | |  |  |  |  |  |
| - | | частичное | |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | способности | | | каналов | | связи, | |  |  |  |  |  | способности | | |  |  |  |  |  |
|  | использование | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | производительности | | | | | сетевых | |  |  |  |  |  | каналов | | связи, | |  |  |  |  |
|  | ресурсов; | |  |  |  |  |  |  |  |  |  |  |  | | |  |
|  |  |  |  |  |  | устройств, | | |  | нарушением | | |  |  |  |  |  | производительно | | | |  |  |  |  |
| - | |  | полное |  |  |  |  |  |  |  |  |  |  |  | | |  |
|  |  |  |  |  | требований | | | к |  | времени | |  |  |  |  |  | сти | сетевых | | |  |  |  |  |
|  | исчерпание | |  |  |  |  |  |  |  |  |  |  |  |  | | |  |
|  |  |  |  |  |  | обработки запросов; | | | |  |  |  |  |  |  |  |  | устройств; | |  |  |  |  |  |  |
|  | ресурсов; | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | - | | исчерпание ресурсов ИСПДн | | | | | |  |  |  |  | - | | снижение | | |  |  |  |  |
| - | | нарушение | |  |  |  |  |  |  |  |  | | |  |
|  |  |  |  | при | | обработке | |  | пакетов, | |  |  |  |  |  | производительно | | | |  |  |  |  |
|  | логической | |  |  |  |  |  |  |  |  |  |  |  |  | | |  |
|  |  |  |  |  |  | передаваемых | | |  |  |  |  |  |  |  |  |  | сти | серверных | | |  |  |  |  |
|  | связности | | между |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | |  |
|  |  |  |  |  | злоумышленником (занятие всей | | | | | | |  |  |  |  |  | приложений; | | |  |  |  |  |  |
|  | техническими | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | полосы | | пропускания | | | каналов | |  |  |  |  |  | - невозможности | | | |  |  |  |  |
|  | средствами | |  |  |  |  |  |  |  |  |  |  |  | | |  |
|  |  |  |  |  |  | связи, | | переполнение | | | очередей | |  |  |  |  |  | передачи | |  |  |  |  |  |  |
|  | ИСПДн; | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | запросов на обслуживание); | | | | | |  |  |  |  |  |  | сообщений | | из-за | |  |  |  |  |
| - | | использование | |  |  |  |  |  |  |  |  |  |  |  | | |  |
|  |  |  | - | | передача | | нарушителем | | | |  |  |  |  |  | отсутствия | |  |  |  |  |  |  |
|  | ошибок | | в |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | управляющих | | | сообщений | | | от |  |  |  |  |  | доступа к | | среде | |  |  |  |  |
|  | программах. | | |  |  |  |  |  |  |  |  |  |  | | |  |
|  |  |  |  |  | имени | | сетевых | | устройств, | | |  |  |  |  |  | передачи, отказ в | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  | | |  |
|  |  |  |  |  |  |  |  | приводящих | | | к | изменению | | |  |  |  |  |  | установлении | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  | маршрутно-адресных | | | | | данных | |  |  |  |  |  | соединения; | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  | или | | идентификационной | | | | и |  |  |  |  |  | отказ |  |  | в |  | | |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Класс угроз |  |  |  | Источник |  |  | Способ реализации | | |  |  |  | Объект |  |  | Нарушаемые | |  |  | Вероятность |  |  |  |
|  |  |  |  |  | угроз |  |  |  |  |  | воздействия |  |  | свойства ИБ | |  |  | реализации |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | аутентификационной | | |  |  |  |  |  |  | предоставлении | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | информации; | |  |  |  |  |  |  |  | сервиса; | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  | - | | передача | пакетов | | с |  | | |  | - невозможности | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | нестандартными | |  | атрибутами | |  | | |  | передачи, | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | или | имеющих | | длину, | |  | | |  | сообщений | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | превышающую | | максимально | | |  | | |  | (получения | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | допустимый размер | | |  |  |  |  |  |  | услуг) | из-за | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | отсутствия | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | корректных | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | маршрутно- | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | адресных | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | данных; | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | - | | нарушения | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | работоспособнос | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | ти | сетевых | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | устройств | | |  |  |  |  |  |

Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы:

1. Используется лицензионное ПО надежных производителей.
   1. При осуществлении взаимодействия с сетью Интернет используются средства межсетевого экранирования.
   2. В ЛВС используются только коммутаторы и маршрутизаторы (хабы не используются).
   3. На рабочих станциях пользователей, функционирующих под управлением ОС версии не ниже Windows 7, устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.
   4. На рабочих станциях установлено антивирусное ПО. Осуществляется регулярное обновление антивирусного ПО. Управление антивирусным ПО осуществляется

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Класс угроз | |  |  | Источник | |  | Способ реализации | | |  |  |  | Объект |  |  |  | Нарушаемые |  |  | Вероятность |  |  |
|  |  |  | угроз |  |  |  |  |  | воздействия | |  |  | свойства ИБ |  |  | реализации |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | централизовано. | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | 6. | | 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. | | | | | | | |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | 2. | | Не используется система обнаружения/предотвращения вторжений. | | | | | | | | | | | | | |  |  |  |  |
|  |  |  |  | 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. | | | | | | |  |  |  |  |  |  |  |  |  |  |  |  |
| 23. | | Угрозы | |  | Внешний | |  | Реализуется путем эксплуатации | | | | |  | Технические | | |  | Нарушение | |  | Высокая | |  |
|  | нарушитель | |  | уязвимостей, | |  | вызванных | |  | средства | ИСПДн | |  | конфиденциальн | |  | вероятность | |  |
|  | удаленного | | |  |  |  |  |  |  |  |
|  |  |  |  |  | некорректными | | | настройками | |  | (каналы | связи), | |  | ости, | |  |  |  |  |
|  | запуска | | |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | операционной | | системы, СУБД, | | | программные | | | |  | целостностии | |  |  |  |  |
|  | приложений, в том | | |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | сетевых | сервисов, | | прикладного | |  | средства ИСПДн | | |  | доступности | |  |  |  |  |
|  | числе: | | |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | ПО |  |  |  |  |  |  |  |  |  | ПДн | |  |  |  |  |
|  | - распространение | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | Использование | | | скрытых | |  |  |  |  |  |  |  |  |  |  |  |
|  | файлов, | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | компонентов | |  | ("троянских" | |  |  |  |  |  |  |  |  |  |  |  |
|  | содержащих | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | программ) | | либо | штатных | |  |  |  |  |  |  |  |  |  |  |  |
|  | несанкционирован | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | средств | управления | | | и |  |  |  |  |  |  |  |  |  |  |  |
|  | ный | исполняемый | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | администрирования | | |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | код; |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | компьютерных сетей | | | |  |  |  |  |  |  |  |  |  |  |  |  |
| - | | переполнение | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы: | | | | | | | | | | | | | | |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Класс угроз | |  |  |  | Источник | |  | Способ реализации |  |  | Объект |  |  | Нарушаемые |  | Вероятность |  |  |  |
|  |  |  |  |  | угроз |  |  |  |  | воздействия |  |  | свойства ИБ |  | реализации |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | буфера | | | 1. | | | Используется лицензионное системное ПО надежных производителей. | | | | | | | | | |  |  |  |  |
|  |  | приложений- | | | 2. | | | На рабочих станциях пользователей, функционирующих под управлением ОС | | | | | | | | | |  |  |  |  |
|  |  | серверов; | | |  |  | версии не ниже Windows 7, устанавливаются обновления и патчи для системного ПО, | | | | | | | | | | |  |  |  |  |
|  | - | | использование | |  |  | сервисов и служб, которые закрывают известные и новые уязвимости. | | | | | | | | | | |  |  |  |  |
|  |  | возможностей | | | 3. | | | На рабочих станциях установлено антивирусное ПО. Осуществляется регулярное | | | | | | | | | |  |  |  |  |
|  |  | удаленного | | |  |  | обновление антивирусного ПО. Управление антивирусным ПО осуществляется | | | | | | | | | | |  |  |  |  |
|  |  | управления | | |  |  | централизовано. | | | | |  |  |  |  |  |  |  |  |  |  |
|  |  | системой | | | 4. | | | Обеспечивается разграничение доступа пользователей к ИСПДн. | | | | | | | | | |  |  |  |  |

1. При осуществлении взаимодействия с сетью Интернет используются средства межсетевого экранирования.
2. При осуществлении удаленного доступа траффик защищается при помощи технологии VPN.
3. 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.
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.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Внешний | Реализуется путем эксплуатации | Программные | Нарушение | Низкая |
|  | нарушитель. | web-уязвимостей | средства ИСПДн | конфиденциальн | вероятность |
|  | Внутренний |  |  | ости, |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Класс угроз |  |  | Источник | |  | Способ реализации | | | |  |  |  | Объект |  |  | Нарушаемые |  |  | Вероятность |  |  |
|  |  |  | угроз |  |  |  |  |  | воздействия |  |  | свойства ИБ |  |  | реализации |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | нарушитель | |  |  |  |  |  |  |  |  |  |  |  | целостности | и |  | | |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | доступности |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | ПДн |  |  |  |  |  |
|  |  |  |  | Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы: | | | | | | | | | | | | | | |  | | |  |
|  |  |  | 1. | | На рабочих станциях установлено антивирусное ПО. Осуществляется регулярное | | | | | | | | | | | | | |  | | |  |
|  |  |  |  | обновление антивирусного ПО. Управление антивирусным ПО осуществляется | | | | | | | | | | | | | | |  | | |  |
|  |  |  |  | централизовано. | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | 2. | | На рабочих станциях пользователей, функционирующих под управлением ОС | | | | | | | | | | | | | |  | | |  |
|  |  |  |  | версии не ниже Windows 7, устанавливаются обновления и патчи для системного ПО, | | | | | | | | | | | | | | |  | | |  |
|  |  |  |  | сервисов и служб, которые закрывают известные и новые уязвимости. | | | | | | | | | | | | | |  |  |  |  |  |
|  |  |  | 3. | | При осуществлении взаимодействия с сетью Интернет используются средства | | | | | | | | | | | | | |  | | |  |
|  |  |  |  | межсетевого экранирования. | | | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 24. Угроза | |  | Внутренний | |  | Реализуется через почтовый или | | | | | |  | Программные |  |  | Нарушение |  |  | Высокая | |  |
|  |  | нарушитель | |  | файловый | обмен. | | | Запись кода | |  | средства ИСПДн |  |  | конфиденциальн | | вероятность | | |  |
|  | внедрения по сети | |  |  |  |  |  |  |
|  | вредоносных | |  |  |  |  | вредоносного ПО в код других | | | | | |  |  |  |  | ости, |  |  |  |  |  |
|  |  |  |  |  | программ | с | целью | | | получения |  |  |  |  | целостности | и |  |  |  |  |
|  | программ | |  |  |  |  |  |  |  |  |  | | |  |
|  |  |  |  |  | управления |  |  | при | | запуске |  |  |  |  | доступности |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | зараженных | | файлов, | | | создание |  |  |  |  | ПДн |  |  |  |  |  |
|  |  |  |  |  |  |  | файлов-двойников | | | |  | для |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | легального |  | ПО, | | копирование | |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | кода вредоносной программы в | | | | | |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | каталоги | для | | последующего | | |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | запуска пользователем | | | | | |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы: | | | | | | | | | | | | | | |  | | |  |
|  |  |  | 1. | | Обеспечивается разграничение доступа пользователей к ИСПДн. | | | | | | | | | | | | |  |  |  |  |  |
|  |  |  | 2. | | На рабочих станциях установлено антивирусное ПО. Осуществляется регулярное | | | | | | | | | | | | | |  | | |  |
|  |  |  |  | обновление | |  | антивирусного | | | ПО. | | Управление | | антивирусным | ПО осуществляется | | | |  | | |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Класс угроз |  |  |  | Источник |  |  | Способ реализации |  |  | Объект |  |  | Нарушаемые |  | Вероятность |  |  |  |
|  |  |  |  |  | угроз |  |  |  |  | воздействия |  |  | свойства ИБ |  | реализации |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

централизовано.

1. На рабочих станциях пользователей, функционирующих под управлением ОС версии не ниже Windows 7, устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.

Факторы, повышающие вероятность реализации угрозы:

1. Пользователи обладают правами локальных администраторов на своих рабочих станциях.
2. В ходе обследования получены данные о низком уровне компьютерной грамотности пользователей вообще и информационной безопасности в частности.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Внешний | Реализуется путем эксплуатации | | Программные | Нарушение | Средняя |
| нарушитель, | уязвимостей, | вызванных | средства ИСПДн | конфиденциальн | вероятность |
| Внутренний | некорректными | настройками |  | ости, |  |
| нарушитель | операционной | системы, СУБД |  | целостностии |  |
|  | или сетевых сервисов | |  | доступности |  |
|  |  |  |  | ПДн |  |
| Применяемые защитные меры, снижающие вероятность и ущерб от реализации угрозы: | | | | |  |

1. Обеспечивается разграничение доступа пользователей к ИСПДн.
   1. На серверах рабочих станциях установлено антивирусное ПО. Осуществляется регулярное обновление антивирусного ПО. Управление антивирусным ПО осуществляется централизовано.
   2. На рабочих станциях пользователей, функционирующих под управлением ОС версии не ниже Windows 7, устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.
   3. При осуществлении удаленного доступа траффик защищается при помощи технологии VPN.

Факторы, повышающие вероятность реализации угрозы: не осуществляется настройка безопасности ОС на рабочих станциях пользователей.

## 10.3. Определение актуальности угроз безопасности ПДн

Результаты определения актуальности угроз безопасности ПДн, обрабатываемых в ИСПДн:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  | Вероятность |  |  |  |  |  | Коэффициент |  |  | Возможность |  |  |  |  |  |  |  |  |
|  | Класс угроз |  |  |  |  |  |  | Y2 |  |  | реализуемости |  |  |  |  | Опасность |  |  | Актуальность |  |  |
|  |  |  |  |  | реализации |  |  |  |  |  |  | реализации |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  | угрозы Y |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Угрозы первого типа | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Угроза НСД с применением стандартных | | | |  | Средняя | | 5 | |  | 0,5 | |  |  | Средняя | |  | Низкая | |  | Неактуальная | |  |
|  | функций операционной системы | | | |  | вероятность | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Угроза НСД с применением специально | | | |  | Средняя | | 5 | |  | 0,5 | |  |  | Средняя | |  | Низкая | |  | Неактуальная | |  |
|  | созданных для этого программ | | |  |  | вероятность | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Угрозы типа «Отказ в обслуживании», в | | | |  | Средняя | | 5 | |  | 0,5 | |  |  | Средняя | |  | Низкая | |  | Неактуальная | |  |
|  | том числе | использование | | известных |  | вероятность | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | уязвимостей в ПО | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Угрозы удаленного запуска приложений, | | | |  | Низкая | | 2 | |  | 0,35 | |  |  | Средняя | |  | Низкая | |  | Неактуальная | |  |
|  | в том числе: |  |  |  |  | вероятность | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | ­ распространение файлов, содержащих | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | несанкционированный | | исполняемый | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | код; |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | ­ переполнение буфера | | приложений- | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | серверов; |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | ­ использование | | возможностей | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | удаленного управления системой. | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Угрозы второго типа | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Угроза НСД с применением стандартных | | | |  | Средняя | | 5 | |  | 0,5 | |  |  | Средняя | |  | Низкая | |  | Неактуальная | |  |
|  | функций прикладного ПО | |  |  |  | вероятность | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Угроза НСД с применением специально | | | |  | Средняя | | 5 | |  | 0,5 | |  |  | Средняя | |  | Низкая | |  | Неактуальная | |  |
|  | созданных для этого программ | | |  |  | вероятность | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Угрозы типа «Отказ в обслуживании», в | | | |  | Низкая | | 2 | |  | 0,35 | |  |  | Средняя | |  | Низкая | |  | Неактуальная | |  |
|  | том числе | использование | | известных |  | вероятность | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| уязвимостей в ПО | |  |  |  |  |  |  |  |  |  |
|  | | | | |  |  |  |  |  |  |
| Угрозы удаленного запуска приложений, | | | | | Низкая | 2 | 0,35 | Средняя | Низкая | Неактуальная |
| в том числе: | |  |  |  | вероятность |  |  |  |  |  |
| ­ распространение файлов, содержащих | | | | |  |  |  |  |  |  |
| несанкционированный | | | | исполняемый |  |  |  |  |  |  |
| код; |  |  |  |  |  |  |  |  |  |  |
| ­ переполнение | | буфера | | приложений- |  |  |  |  |  |  |
| серверов; | |  |  |  |  |  |  |  |  |  |
| ­ использование | |  |  | возможностей |  |  |  |  |  |  |
| удаленного управления системой. | | | | |  |  |  |  |  |  |
| Угрозы третьего типа | | |  |  |  |  |  |  |  |  |
| Угрозы утечки акустической (речевой) | | | | | Маловероятн | 0 | 0,25 | Низкая | Низкая | Неактуальная |
| информации | |  |  |  | ая угроза |  |  |  |  |  |
| Угрозы утечки видовой информации | | | | | Низкая | 2 | 0,35 | Средняя | Низкая | Неактуальная |
|  |  |  |  |  | вероятность |  |  |  |  |  |
|  |  |  |  |  | Низкая | 2 | 0,35 | Средняя | Низкая | Неактуальная |
|  |  |  |  |  | вероятность |  |  |  |  |  |
| Угрозы утечки информации по каналам | | | | | Низкая | 2 | 0,35 | Средняя | Низкая | Неактуальная |
| ПЭМИН | |  |  |  | вероятность |  |  |  |  |  |
| Угрозы | модификации | | базовой системы | | Средняя | 5 | 0,5 | Средняя | Низкая | Неактуальная |
| ввода/вывода | | (BIOS), | | перехвата | вероятность |  |  |  |  |  |
| управления загрузкой, перехвата или | | | | |  |  |  |  |  |  |
| подбора паролей или идентификаторов, а | | | | |  |  |  |  |  |  |
| также | использование | | технологических | |  |  |  |  |  |  |
| паролей BIOS | |  |  |  |  |  |  |  |  |  |
| Угроза НСД с применением стандартных | | | | | Высокая | 10 | 0,75 | Высокая | Низкая | Актуальная |
| функций операционной системы, СУБД, | | | | | вероятность |  |  |  |  |  |
| прикладной программы | | |  |  |  |  |  |  |  |  |
| Угроза НСД с применением специально | | | | | Высокая | 10 | 0,75 | Высокая | Низкая | Актуальная |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |
| созданных для этого программ | | |  | вероятность |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| Угроза | утечки | информации | путем | Высокая | 10 | 0,75 | Высокая | Низкая | Актуальная |  |  |
| преднамеренного копирования доступных | | | | вероятность |  |  |  |  |  |  |  |
| ПДн на неучтенные (в том числе | | | |  |  |  |  |  |  |  |  |
| отчуждаемые) носители, а также печать | | | |  |  |  |  |  |  |  |  |
| неучтенных копий документов с ПДн на | | | |  |  |  |  |  |  |  |  |
| принтерах | |  |  |  |  |  |  |  |  |  |  |
| Угроза внедрения вредоносных программ | | | | Высокая | 10 | 0,75 | Высокая | Низкая | Актуальная |  |  |
| с использованием съемных носителей, а | | | | вероятность |  |  |  |  |  |  |  |
| также в связи с подключением стороннего | | | |  |  |  |  |  |  |  |  |
| оборудования | | (компьютеров, | КПК, |  |  |  |  |  |  |  |  |
| смартфонов, телефонов, фотоаппаратов, | | | |  |  |  |  |  |  |  |  |
| видеокамер,флэш-дисковииных | | | |  |  |  |  |  |  |  |  |
| устройств, в том числе имеющих выход в | | | |  |  |  |  |  |  |  |  |
| беспроводные сети связи) | | |  |  |  |  |  |  |  |  |  |
| Угроза «Анализа сетевого трафика» | | |  | Высокая | 10 | 0,75 | Высокая | Низкая | Актуальная |  |  |
|  |  |  |  | вероятность |  |  |  |  |  |  |  |
| Угроза сканирования сети | | |  | Высокая | 10 | 0,75 | Высокая | Низкая | Актуальная |  |  |
|  |  |  |  | вероятность |  |  |  |  |  |  |  |
| Угроза выявления паролей | | |  | Высокая | 10 | 0,75 | Высокая | Низкая | Актуальная |  |  |
|  |  |  |  | вероятность |  |  |  |  |  |  |  |
| Угроза | навязывания ложного маршрута | | | Средняя | 5 | 0,5 | Средняя | Низкая | Неактуальная |  |  |
| сети |  |  |  | вероятность |  |  |  |  |  |  |  |
| Угроза внедрения ложного объекта сети | | | | Средняя | 5 | 0,5 | Средняя | Низкая | Неактуальная |  |  |
|  |  |  |  | вероятность |  |  |  |  |  |  |  |
| Угрозы типа «Отказ в обслуживании», в | | | | Средняя | 5 | 0,5 | Средняя | Низкая | Неактуальная |  |  |
| том числе: | |  |  | вероятность |  |  |  |  |  |  |  |

* частичное использование ресурсов;
* полное исчерпание ресурсов;

­ нарушение логической связности

между техническим средствами

ИСПДн;

* использование ошибок в программах.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Угрозы удаленного запуска приложений, | | | Высокая | 10 | 0,75 | Высокая | Низкая |  | Актуальная |  |  |
| в том числе: |  |  | вероятность |  |  |  |  |  |  |  |  |
| ­ распространение файлов, содержащих | | |  |  |  |  |  |  |  |  |  |
| Низкая | 2 | 0,35 | Средняя | Низкая |  | Неактуальная |  |  |
| несанкционированный | | исполняемый |  |  |  |
| вероятность |  |  |  |  |  |  |  |  |
| код; |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| ­ переполнение | буфера | приложений- |  |  |  |  |  |  |  |  |  |
| серверов; |  |  |  |  |  |  |  |  |  |  |  |
| ­ использование |  | возможностей |  |  |  |  |  |  |  |  |  |
| удаленного управления системой. | | |  |  |  |  |  |  |  |  |  |
| Угроза внедрения | по сети | вредоносных | Высокая | 10 | 0,75 | Высокая | Низкая |  | Актуальная |  |  |
| программ |  |  | вероятность |  |  |  |  |  |  |  |  |
|  |  |  | Средняя | 5 | 0,5 | Средняя | Низкая |  | Неактуальная |  |  |
|  |  |  | вероятность |  |  |  |  |  |  |  |  |

Заключение

Целью данного проекта была реализация модели угроз обработки ПДН в ИСПДН.

В результате практической работы над проектом получено следующее:

1. Изучены следующие ИСПДН: 1С Бухгалтерия 8.3, 1C ЗИК 8.3, Рабочие станции пользователей, distance.learning.ru, Портал ДПО и Active Directory;
2. Разработаны модели угроз ПДн для следующих ИСПДН: Рабочие станции пользователей, Active Directory, distance.learining.ru и Портал ДПО;
3. Для всех ИСПДН,для которых была разработана модель угроз,были определены следующие параметры:
   1. Уровень исходной защищенности ИСПДН
   2. Описание угроз безопасности ПДн
   3. Определение актуальности угроз безопасности ПДн