МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(дипломная работа)

На тему «Методика предотвращения рисков информационной безопасности в распределенных информационных системах»

Исполнитель Цветков Александр Александрович
(фамилия,имя,отчество)

Руководитель Грызунов Виталий Владимирович
(фамилия, имя, отчество)

«К защите допускаю»

Заведующий кафедрой_____

(подпись)

_____
(ученаястепень,ученое звание)

_____ Бурлов В.Г._____
(фамилия,имя,отчество)

«» 23г

Санкт–Петербург

2023

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В наши дни достаточно распространены распределенные информационные системы, топология которых сильно развита. Разные части системы выполняют различные задачи. Из-за большого количества узлов и связей в таких системах, а также данных, которые они обрабатывают, возникает большое количество рисков информационной безопасности.

Актуальность темы дипломной работы определяется высоким уровнем рисков компрометации, краже, продаже и распространения информации, составляющей персональные данные, даже в условиях стремительного роста технологий и инструментальной базы для защиты информации. Невозможно обеспечить стопроцентный уровень защиты распределённых информационных систем, при этом корректно расставляя приоритеты в задачах по защите данных. Надежная защита вычислительной и сетевой инфраструктуры является базовой задачей в области информационной безопасности для любой организации работающей с данными ограниченными для общего доступа.

В настоящее время компании малого и среднего бизнеса, а также государственные организации обязаны в соответствии с действующим законодательством организовывать защиту персональных данных населения. Защита персональных данных обеспечивается различными методами и средствами, обеспечивающими безопасность, целостность и конфиденциальность данных.

Документ, регламентирующий средства защиты персональных данных был разработанный ФСТЭК и утверждён в 2013 году, в данной работе будет рассмотрены приведенные в нём требования на предмет актуальности на сегодняшний день.

В нашей стране утверждены различные законы и приказы описывающие требования к информационной безопасности персональных данных, так же есть различные методы и способы защиты информации.

Предметом исследования в дипломной работе является распределенная информационная система, одной из задач которой является обработка персональных данных.

Целью дипломной работы является: снижение рисков информационной безопасности в распределённых информационных системах.

Задачи поставленные для достижения цели:

- Описать особенности организации с точки зрения информационной безопасности

- Проанализировать текущие методы предотвращения рисков информационной безопасности в информационных системах

- Подготовить стенд для моделирования угроз на рассматриваемую систему

- Смоделировать поведение системы, при воздействии выбранных атак

- Опросить экспертов в сфере информационной безопасности для получения статистических данных

- Произвести расчёты и анализ полученных результатов

- Проверка предлагаемых методиками средств защиты

ГЛАВА 1. ОПИСАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1.1 Особенности распределённой информационной системы

Распределенная информационная система - это набор интерактивных программных модулей, представляющих единую систему пользователей. Фактически, любая система, которая совместно обрабатывает данные между двумя или более компьютерами, является распределенной вычислительной системой. Он используется для снижения нагрузки на сервер и обеспечения нормальной работы удаленного отдела.

- Каждый узел распределенной системы должен быть независимым или автономным.

- Локальная независимость означает, что все узлы распределенной системы имеют равные права, то есть они считаются равными. Это означает, что нет необходимости вызывать так называемый центральный узел или главный узел для доступа к каким-либо централизованным службам.

- Непрерывность работы.

- Независимо от местоположения.

- Когда текущая переменная может быть разложена на фрагменты в реальном сохраненном процессе, система должна обеспечить независимость от фрагментов.

- Система должна поддерживать репликацию данных, когда сохраненные переменные могут быть отражены набором отдельных копий или копиями, хранящимися на разных локальных узлах.

- Возможность обработки распределенных запросов

- Аппаратная независимость.

- Не зависит от сети.

1.2 Особенности с точки зрения защиты персональных данных при их обработке

1) Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или

обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных:

- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных

- применением организационных и технических мерпо обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнениятребованийк защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных

- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации

- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных

- учетом машинных носителей персональных данных

- обнаружением фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них

- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним

- установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных

- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных

2) Правительство Российской Федерации с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливает:

- уровни защищенностиперсональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных

- требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных

- требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

- Состав и содержание необходимых для выполнения установленных Правительством Российской Федерации в соответствии с частью 3 настоящей статьи требований к защите персональных данных для каждого из уровней защищенности, организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

- Федеральные органы исполнительной власти, осуществляющие функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности, органы государственной

власти субъектов Российской Федерации, Банк России, органы государственных внебюджетных фондов, иные государственные органы в пределах своих полномочий принимают нормативные правовые акты, в которых определяют угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки.

- Наряду с угрозами безопасности персональных данных, определенных в нормативных правовых актах, принятых в соответствии с частью 5 настоящей статьи, ассоциации, союзы и иные объединения операторов своими решениями вправе определить дополнительные угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с учетом содержания персональных данных, характера и способов их обработки.

- Проекты нормативных правовых актов, указанных в части 5 настоящей статьи, подлежат согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации. Проекты решений, указанных в части 6 настоящей статьи, подлежат согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в порядке, установленном Правительством Российской Федерации. Решение федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, и федерального органа исполнительной власти, уполномоченного в области противодействия

техническим разведкам и технической защиты информации, об отказе в согласовании проектов решений, указанных в части 6 настоящей статьи, должно быть мотивированным.

- Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при обработке персональных данных в государственных информационных системах персональных данных осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

- Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, решением Правительства Российской Федерации с учетом значимости и содержания обрабатываемых персональных данных могут быть наделены полномочиями по контролю за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при их обработке в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности и не являющихся государственными информационными системами персональных данных, без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

- Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой

технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

- Для целей настоящей статьи под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных. Под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

- Оператор обязан в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование его о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных.

- Указанная в части 12 настоящей статьи информация (за исключением информации, составляющей государственную тайну) передается федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, в уполномоченный орган по защите прав субъектов персональных данных.

- Порядок передачи информации в соответствии с частью 13 настоящей статьи устанавливается совместно федеральным органом

исполнительной власти, уполномоченным в области обеспечения безопасности, и уполномоченным органом по защите прав субъектов персональных данных [1].

1.3 Особенности объекта исследования

В качестве объекта исследования была выбрала компания с названием «СофтИнформ».

Штат предприятия составляет 150 сотрудников. В компании присутствуют несколько отделов, каждый из которых осуществляет свою деятельность. В данной работе нас будет интересовать отдел экономики и финансов, который включает в себя 3 автоматизированных рабочих места на которых происходит обработка и хранение персональных данных представлена на рисунок 1, которые в свою очередь включены в общую локальную сеть предприятия, имеющую выход в сеть Internet . Именно на этом отделе мы в дальнейшем будем проводить исследование.

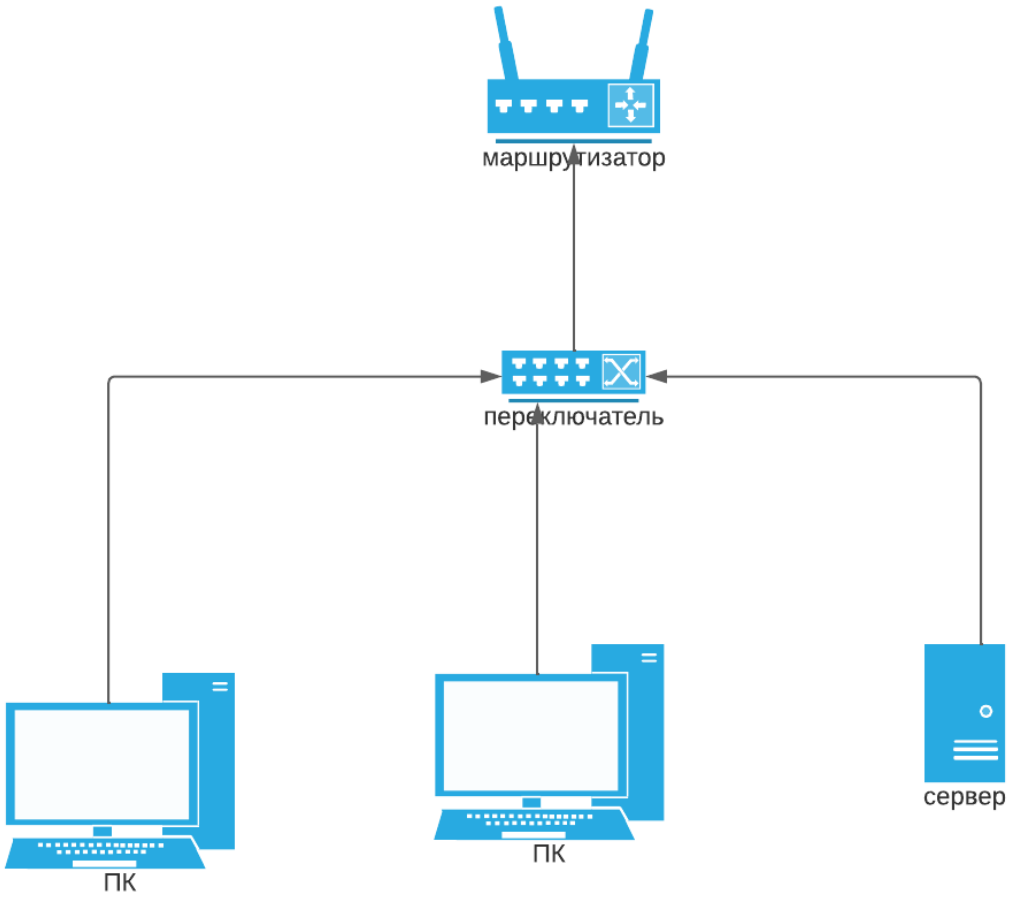

Рисунок 1. Схема отдела экономики и финансов

Деятельность организации связана с использованием вычислительной техники и информационных технологий, в неё входит:

- Испытания на соответствие требованиям защищенности от несанкционированного доступа к информации

- Анализ уязвимостей и контроль отсутствия не декларированных возможностей в программном обеспечении

- Разработка и внедрение систем защиты информации, составляющей государственную тайну, на основе сертифицированных базовых информационных защищенных компьютерных технологий

В перечень активов организации входит:

- Оборудование – оценочная стоимость 75000000 рублей

- Денежные средства – 57000000 рублей

- Рыночные ценные бумаги 25000000 рублей

- Здания, сооружения – оценочная стоимость 185000000 рублей

- Торговые марки – оценочная стоимость 20000000 рублей

- Программные продукты – оценочная стоимость 60000000 рублей

Модель обработки персональных данных представлена на рисунке 2.

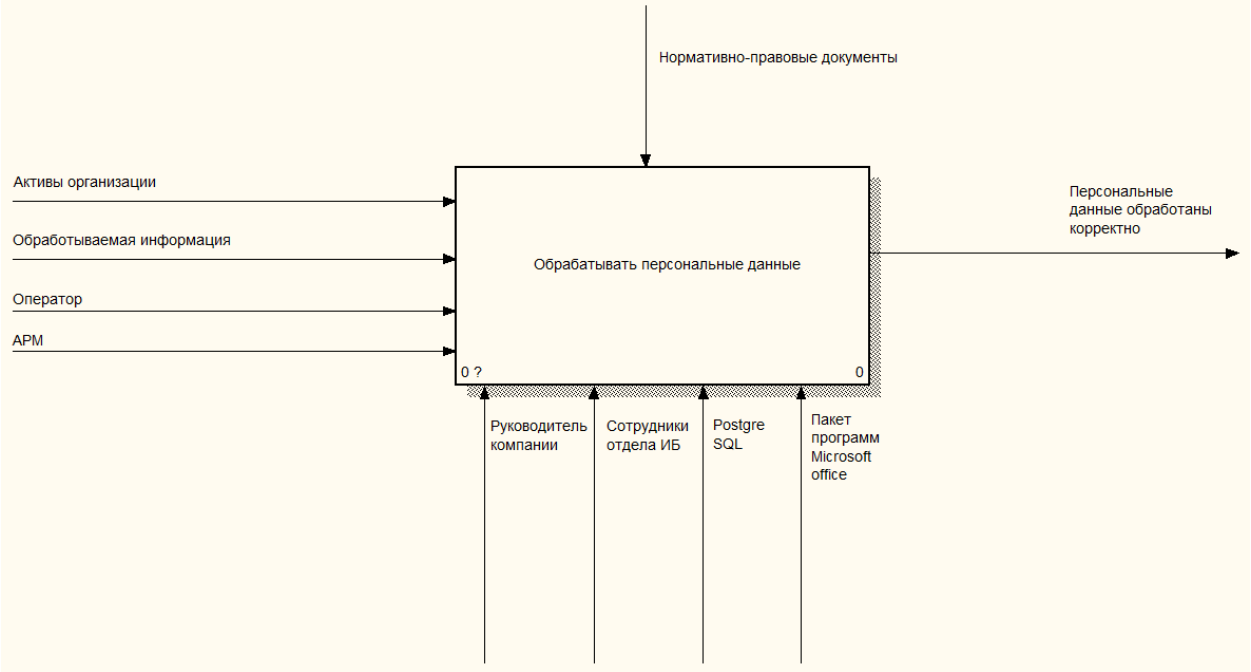

Рисунок 2. Модель процесса обработки ПДн

1.4. Модель угроз

1.4.1 Модель угроз безопасности персональных данных, обрабатываемых в распределенных информационных системах персональных данных

Описание существующихугроз информационной безопасности, их актуальности, возможности реализации и последствий [2].

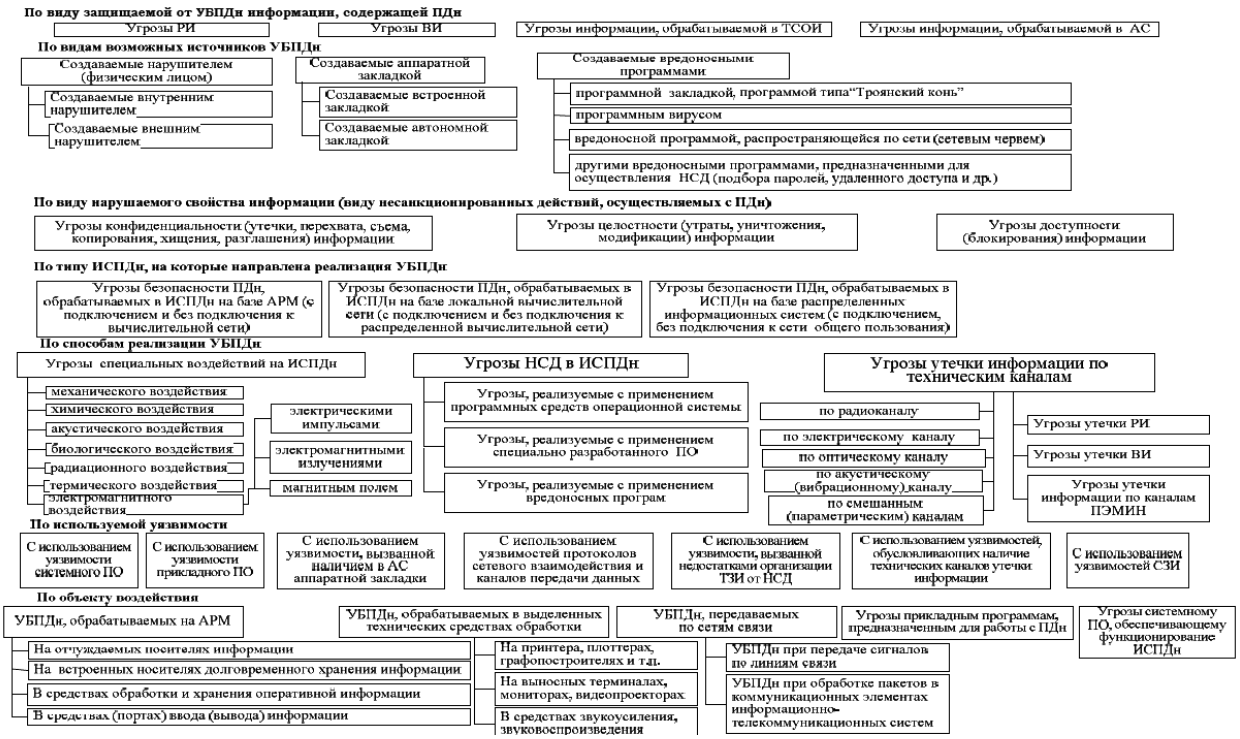

Рисунок 3. Классификация угроз ПНД

При обработке ПДн в распределенных ИСПДн, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена, возможна реализация следующих УБПДн, рисунок 3:

- угрозы утечки информации по техническим каналам;

Основными элементами описания угроз утечки информации по техническим каналам (ТКУИ) являются: источник угрозы, среда (путь) распространения информативного сигнала и носитель защищаемой информации. Источниками угроз утечки информации по техническим каналам являются физические лица, не имеющие доступа к ИСПДн, а также зарубежные спецслужбы или организации (в том числе

конкурирующие или террористические), криминальные группировки, осуществляющие перехват (съем) информации с использованием технических средств ее регистрации, приема или фотографирования. Среда распространения информативного сигнала – это физическая среда, по которой информативный сигнал может распространяться и приниматься (регистрироваться) приемником. Среда распространения может быть как однородной (например, только воздушной), так и неоднородной за счет перехода сигнала из одной среды в другую (например, в результате акустоэлектрических или виброакустических преобразований). Носителем ПДн является пользователь ИСПДн, осуществляющий голосовой ввод ПДн в ИСПДн, акустическая система ИСПДн, воспроизводящая ПДн, а также технические средства ИСПДн и ВТСС, создающие физические поля, в которых информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин. При обработке ПДн в ИСПДн за счет реализации технических каналов утечки информации возможно возникновение следующих УБПДн: угроз утечки акустической (речевой) информации; угроз утечки видовой информации; угроз утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН).

- угрозы НСД к ПДн, обрабатываемым на автоматизированном рабочем месте.

- Угрозы утечки информации по техническим каналам включают в себя:

- угрозы утечки акустической (речевой) информации [3];

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, при обработке ПДн в ИСПДн, обусловлено наличием функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн. Перехват акустической (речевой)

информации в данных случаях возможен с использованием аппаратуры, регистрирующей акустические (в воздухе) и виброакустические (в упругих средах) волны, а также электромагнитные (в том числе оптические) излучения и электрические сигналы, модулированные информативным акустическим сигналом, возникающие за счет преобразований в технических средствах обработки ПДн, ВТСС и строительных конструкциях и инженерно-технических коммуникациях под воздействием акустических волн. Кроме этого, перехват акустической (речевой) информации возможен с использованием специальных электронных устройств съема речевой информации, внедренных в технические средства обработки ПДн, ВТСС и помещения или подключенных к каналам связи. Угрозы безопасности ПДн, связанные с перехватом акустической информации с использованием специальных электронных устройств съема речевой информации («закладочных устройств»), определяются в соответствии с нормативным документами Федеральной службы безопасности Российской Федерации в установленном ею порядке. Перехват акустической (речевой) информации может вестись:
стационарной аппаратурой, размещаемой в близлежащих строениях (зданиях) с неконтролируемым пребыванием посторонних лиц;
портативной возимой аппаратурой, размещаемой в транспортных средствах, осуществляющих движение вблизи служебных помещений или при их парковке рядом с этими помещениями; портативной носимой аппаратурой – физическими лицами при их неконтролируемом пребывании в служебных помещениях или в непосредственной близости от них;
автономной автоматической аппаратурой, скрытно устанавливаемой физическими лицами непосредственно в служебных помещениях или в непосредственной близости от них.

- 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, информационновычислительных 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. Угрозы безопасности ПДн, связанные с их перехватом при использовании специальных электронных устройств съема видовой информации (видеозакладок), определяются в соответствии с нормативным документами Федеральной службы безопасности Российской Федерации в установленном ею порядке. Необходимым условием осуществления просмотра (регистрации) ПДн является наличие прямой видимости между средством наблюдения и носителем ПДн. Перехват ПДн может вестись: стационарной аппаратурой, размещаемой в близлежащих строениях (зданиях) с неконтролируемым пребыванием посторонних лиц; портативной возимой аппаратурой, размещаемой в транспортных средствах, осуществляющих движение вблизи служебных помещений или при их парковке рядом с этими помещениями; портативной носимой аппаратурой – физическими лицами при их неконтролируемом пребывании в служебных помещениях или в непосредственной близости от них. 19 Перехват (просмотр) ПДн может осуществляться посторонними лицами путем их непосредственного наблюдения в служебных помещениях либо с расстояния прямой видимости из-за пределов ИСПДн с использованием оптических (оптикоэлектронных) средств.

- угрозы утечки информации по каналу 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 ПД 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, обрабатывающих ПДн (в средствах вычислительной техники, информационно-вычислительных комплексах и сетях, средствах и системах передачи, приема и обработки ПДн, в том числе в 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. Кроме этого, перехват ПЭМИН возможен с использованием электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки ПДн. Регистрация ПЭМИН может вестись с использованием аппаратуры следующих видов: стационарной аппаратурой, размещаемой в близлежащих строениях (зданиях) с неконтролируемым пребыванием посторонних лиц; портативной возимой аппаратуры, размещаемой в транспортных средствах, осуществляющих движение вблизи служебных помещений или при их парковке рядом с этими помещениями; портативной носимой аппаратурой – физическими лицами в непосредственной близости от ИСПДн; автономной автоматической аппаратурой, скрытно устанавливаемой физическими лицами в непосредственной близости от ИСПДн. 20 Каналы утечки информации, обусловленные наводками,

образуются за счет соединительных линий технических средств ИСПДн и ВТСС и посторонних проводников (в том числе цепей электропитания и заземления). Наводки электромагнитных излучений технических средств ИСПДн возникают при излучении элементами технических средств ИСПДн информативных сигналов при наличии емкостной, индуктивной или гальванической связей соединительных линий технических средств ИСПДн, линий ВТСС и посторонних проводников. В результате на случайных антеннах (цепях ВТСС или посторонних проводниках) наводится информативный сигнал. Прохождение информативных сигналов в цепи электропитания возможно при наличии емкостной, индуктивной или гальванической связи источника информативных сигналов в составе технических средств ИСПДн и цепей питания. Прохождение информативных сигналов в цепи заземления обусловлено наличием емкостной, индуктивной или гальванической связи источника информативных сигналов в составе аппаратуры ТСПИ и цепей заземления. Для съема информации с проводных линий могут использоваться: средства съема сигналов, содержащих защищаемую информацию, с цепей технических средств ИСПДн и ВТСС, линий связи и передачи данных, выходящих за пределы служебных помещений (эквиваленты сети, токовые трансформаторы, пробники); средства съема наведенных информативных сигналов с цепей электропитания; средства съема наведенных информативных сигналов с шин заземления; средства съема наведенных информативных сигналов с проводящих инженерных коммуникаций. Для волоконно-оптической системы передачи данных угрозой утечки информации является утечка оптического излучения, содержащего защищаемую информацию, с боковой поверхности оптического волокна. Появление новых каналов связи – сотовой связи, пейджинговых сообщений, спутниковых и беспроводных сетей передачи данных – привело к развитию специализированных систем и средств контроля и перехвата информации, ориентированных на используемые в них

информационные технологии, в том числе средств: перехвата пейджинговых сообщений и сотовой связи; перехвата информации в каналах передачи данных вычислительных сетей.

- Угрозы НСД связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн, а также нарушителей, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена.

- Угрозы НСД, связанные с действиями нарушителей, имеющих доступ к ИСПДн, аналогичны тем, которые имеют место в распределенных ИСПДн, не имеющей подключения к сетям общего пользования. Кроме того, в такой ИСПДн имеют место угрозы, реализуемые с использованием протоколов межсетевого взаимодействия из внешних сетей, в том числе:

- угрозы "Анализа сетевого трафика" с перехватом передаваемой из ИСПДн и принимаемой в ИСПДн из внешних сетей информации;

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. В ходе реализации угрозы нарушитель изучает логику работы сети – то есть стремится получить однозначное соответствие событий, происходящих в системе, и команд, пересылаемых при этом хостами, в момент появления данных событий. В дальнейшем это позволяет злоумышленнику на основе задания соответствующих команд получить, например, привилегированные права на действия в системе или расширить свои полномочия в ней, перехватить поток передаваемых данных, которыми обмениваются компоненты сетевой операционной системы, для извлечения конфиденциальной или идентификационной информации (например, статических паролей пользователей для доступа к удаленным хостам по

протоколам FTP и TELNET, не предусматривающим шифрование), ее подмены, модификации и т.п.

- угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.;

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

- угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;

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

- угрозы подмены доверенного объекта;

Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа. Такая угроза эффективно реализуется в системах, где применяются нестойкие алгоритмы идентификации и аутентификации хостов, пользователей и т.д.

Под доверенным объектом понимается объект сети (компьютер, межсетевой экран, маршрутизатор и т.п.), легально подключенный к серверу. Могут быть выделены две разновидности процесса реализации указанной угрозы: с установлением и без установления виртуального соединения. Процесс реализации с установлением виртуального соединения состоит в присвоении прав доверенного субъекта взаимодействия, что позволяет нарушителю вести сеанс работы с объектом сети от имени доверенного субъекта. Реализация угрозы данного типа требует преодоления системы идентификации и аутентификации сообщений (например, атака rsh-службы UNIX-хоста). Процесс реализации угрозы без установления виртуального соединения может иметь место в сетях, осуществляющих идентификацию передаваемых сообщений только по сетевому адресу отправителя. Сущность заключается в передаче служебных сообщений от имени сетевых управляющих устройств (например, от имени маршрутизаторов) об изменении маршрутно-адресных данных. При этом необходимо иметь в виду, что единственными идентификаторами абонентов и соединения (по протоколу TCP) являются два 32-битных параметра Initial Sequence Number – ISS (номер последовательности) и Acknowledgment Number – ACK (номер подтверждения). Следовательно, для формирования ложного TCP-пакета нарушителю необходимо знать текущие идентификаторы для данного соединения – ISSa и ISSb, где: ISSa – некоторое численное значение, характеризующее порядковый номер отправляемого TCP-пакета, устанавливаемого TCP-соединения, инициированного хостом A; ISSb – некоторое численное значение, характеризующее порядковый номер отправляемого TCP-пакета, устанавливаемого TCP-соединения, инициированного хостом B. Значение ACK (номера подтверждения установления TCP-соединения) определяется как значение номера, полученного от респондента ISS (номер последовательности) плюс единица ACKb = ISSa+1. В результате реализации угрозы нарушитель получает

права доступа, установленные его пользователем для доверенного абонента, к техническому средству ИСПДн – цели угроз.

- угрозы навязывания ложного маршрута путем несанкционированного доступа

Данная угроза реализуется одним из двух способов: путем внутрисегментного или межсегментного навязывания. 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 изменения маршрутно-адресных данных как внутри сети, так и во внешних сетях;

- 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.

- 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. Могут быть выделены несколько разновидностей таких угроз: а) 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 ко времени обработки запросов. Примерами реализации угроз подобного рода могут служить: направленный шторм эхо-запросов по протоколу ICMP (Ping flooding), шторм запросов на установление TCP-соединений (SYN-flooding), шторм запросов к FTP-серверу; б) явный отказ в обслуживании, вызванный 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); в) 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; г) явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа «Land», «TearDrop», «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 к 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 полную остановку компьютера из-за невозможности системы заниматься ничем другим, кроме обработки запросов.

- угрозы удаленного запуска приложений;

Угроза заключается в стремлении запустить на хосте ИСПДн различные предварительно внедренные вредоносные программы: программы-закладки, 45 вирусы, «сетевые шпионы», основная цель которых – 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 данных угроз: 1) распространение файлов, содержащих несанкционированный исполняемый код; 2) удаленный запуск приложения путем переполнения буфера приложений-серверов; 3) удаленный запуск приложения путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками либо используемыми штатными средствами. Типовые угрозы первого из указанных подклассов 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. При угрозах второго подкласса используются недостатки программ, реализующих сетевые сервисы (в частности, отсутствие контроля переполнения 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». При угрозах третьего подкласса нарушитель использует возможности удаленного управления системой, предоставляемые скрытыми компонентами (например, «троянскими» программами типа Back Orifice, Net Bus) либо штатными средствами управления и администрирования компьютерных сетей (Landesk Management Suite, Managewise, Back Orifice и т. п.). В результате их использования удается добиться удаленного контроля над станцией в сети. Схематично основные этапы работы этих программ выглядят следующим образом: инсталляция в памяти; ожидание запроса с удаленного хоста, на котором запущена клиентпрограмма, и обмен с ней сообщениями о готовности; передача перехваченной информации клиенту или предоставление ему контроля над атакуемым компьютером.

- угрозы внедрения по сети вредоносных программ.

Возможные последствия от реализации атак представлены на рисунке 4, а правила отнесения угрозы безопасности ПДн к актуальной на рисунке 5.

Возможные последствия реализации угроз различных классов

№ п/п	Тип атаки		Возможные последствия
1	Анализ сетевого трафика		Исследование характеристик сетевого трафика, перехват передаваемых данных, в том числе идентификаторов и паролей пользователей
2	Сканирование сети		Определение протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, активных сетевых сервисов, идентификаторов и паролей пользователей
3	«Парольная» атака		Выполнение любого деструктивного действия, связанного с получением несанкционированного доступа
4	Подмена доверенного объекта сети		Изменение трассы прохождения сообщений, несанкционированное изменение маршрутно-адресных данных. Несанкционированный доступ к сетевым ресурсам, навязывание ложной информации
5	Навязывание ложного маршрута		Несанкционированное изменение маршрутно-адресных данных, анализ и модификация передаваемых данных, навязывание ложных сообщений
6	Внедрение ложного объекта сети		Перехват и просмотр трафика. Несанкционированный доступ к сетевым ресурсам, навязывание ложной информации
7	Отказ в обслуживании	Частичное исчерпание ресурсов	Снижение пропускной способности каналов связи, производительности сетевых устройств. Снижение производительности серверных приложений
		Полное исчерпание ресурсов	Невозможность передачи сообщений из-за отсутствия доступа к среде передачи, отказ в установлении соединения. Отказ в предоставлении сервиса (электронной почты, файлового и т.д.)
		Нарушение логической связности между атрибутами, данными, объектами	Невозможность передачи, сообщений из-за отсутствия корректных маршрутно-адресных данных. Невозможность получения услуг ввиду несанкционированной модификации идентификаторов, паролей и т.п.
		Использование ошибок в программах	Нарушение работоспособности сетевых устройств
8	Удаленный запуск приложений	Путем рассылки файлов, содержащих деструктивный исполняемый код, вирусное заражение	Нарушение конфиденциальности, целостности, доступности информации
		Путем переполнения буфера серверного приложения	
		Путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками либо используемыми штатными средствами	Скрытое управление системой

Рисунок 4. Возможные последствия реализации угроз различных классов

Правила отнесения угрозы безопасности ПДн к актуальной

Возможность реализации угрозы	**Показатель опасности угрозы**		
	Низкая	**Средняя**	**Высокая**
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Рисунок 5. Правила отнесения угрозы безопасности ПДн к актуальной

1.4.2 Модель нарушителя

Представляет собой совокупность сведений о численности, оснащенности, подготовленности, осведомленности, а также действий потенциальных нарушителей.

С точки зрения наличия права постоянного или разового доступа в контролируемую зону (КЗ) объектов размещения ИСПДн все физические лица могут быть отнесены к следующим двум категориям:

- категория I – лица, не имеющие права доступа в контролируемую зону ИСПДн;

- категория II – лица, имеющие право доступа в контролируемую зону ИСПДн.

Все потенциальные нарушители подразделяются на:

- внешних нарушителей, осуществляющих атаки из-за пределов контролируемой зоны ИСПДн;

- внутренних нарушителей, осуществляющих атаки, находясь в пределах контролируемой зоны ИСПДн.

В качестве внешнего нарушителя кроме лиц категории I должны рассматриваться также лица категории II, находящиеся за пределами КЗ.

В отношении ИСПДн в качестве внешнего нарушителями из числа лиц категории I могут выступать:

- бывшие сотрудники Организации; - посторонние лица, пытающиеся получить доступ к ПДн в инициативном порядке;

- представители преступных организаций.

Внешний нарушитель может осуществлять:

- перехват обрабатываемых техническими средствами ИСПДн ПДн за счет их утечки по ТКУИ с использованием портативных, возимых, носимых, а также автономных автоматических средств разведки серийной разработки;

- деструктивные воздействия через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизация, сопровождение, ремонт, утилизация) оказываются за пределами КЗ;

- несанкционированный доступ к информации с использованием специальных программных воздействий посредством программы вирусов, вредоносных программ, алгоритмических или программных закладок;

- перехват информации, передаваемой по сетям связи общего пользования или каналам связи, не защищенным от несанкционированного доступа (НСД) к информации организационно- техническими мерами;

- атаки на ИСПДн путем реализации угроз удаленного доступа.

Внутренний нарушитель (лица категории II) подразделяется на восемь групп в зависимости от способа и полномочий доступа к информационным ресурсам (ИР) ИСПДн.

1. К первой группе относятся сотрудники предприятий, не являющиеся зарегистрированными пользователями и не допущенные к ИР ИСПДн, но имеющие санкционированный доступ в КЗ. К этой категории нарушителей относятся сотрудники различных структурных подразделений предприятий: энергетики, сантехники, уборщицы, сотрудники охраны и другие лица, обеспечивающие нормальное функционирование объекта информатизации.

Лицо данной группы может:

- располагать именами и вести выявление паролей зарегистрированных пользователей ИСПДн;

- изменять конфигурацию технических средств обработки ПДн, вносить программно-аппаратные закладки в ПТС ИСПДн и обеспечивать съем информации, используя непосредственное подключение к техническим средствам обработки информации.

2. Ко второй группе относятся зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ИР ИСПДн с рабочего места. К этой категории относятся сотрудники предприятий, имеющие право доступа к локальным ИР ИСПДн для выполнения своих должностных обязанностей.

Лицо данной группы:

- обладает всеми возможностями лиц первой категории;

- знает, по меньшей мере, одно легальное имя доступа;

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающим доступ к ИР ИСПДн;

- располагает ПДн, к которым имеет доступ.

3. К третьей группе относятся зарегистрированные пользователи подсистем ИСПДн, осуществляющие удаленный доступ к ПДн по локальной сети Организации.

Лицо данной группы:

- обладает всеми возможностями лиц второй категории;

- располагает информацией о топологии сети ИСПДн и составе технических средств ИСПДн;

- имеет возможность прямого (физического) доступа к отдельным техническим средствам (ТС) ИСПДн.

4. К четвертой группе относятся зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента (фрагмента) ИСПДн.

Лицо данной группы:

- обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте ИСПДн;

- обладает полной информацией о технических средствах и конфигурации сегмента ИСПДн;

- имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте ИСПДн;

- имеет доступ ко всем техническим средствам сегмента ИСПДн;

- обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента ИСПДн.

5. К пятой группе относятся зарегистрированные пользователи с полномочиями системного администратора, выполняющего конфигурирование и управление программным обеспечением и оборудованием, включая оборудование, отвечающее за безопасность защищаемого объекта: средства мониторинга, резервного копирования, антивирусного контроля, защиты от несанкционированного доступа.

Лицо данной группы:

- обладает полной информацией о системном, специальном и прикладном ПО, используемом в ИСПДн;

- обладает полной информацией о ТС и конфигурации ИСПДн - имеет доступ ко всем ТС ИСПДн и данным;

- обладает правами конфигурирования и административной настройки ТС ИСПДн.

6. К шестой группе относятся зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности Организации, отвечающего за соблюдение правил разграничения доступа, за генерацию ключевых элементов, смену паролей, криптографическую защиту информации. Администратор безопасности осуществляет аудит тех же средств защиты объекта, что и системный администратор.

Лицо данной группы:

- обладает полной информацией об ИСПДн;

- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;

- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

7. К седьмой группе относятся лица из числа программистов - разработчиков сторонней организации, являющихся поставщиками ПО и лица, обеспечивающие его сопровождение на объекте размещения ИСПДн.

Лицо данной группы:

- обладает информацией об алгоритмах и программах обработки информации в ИСПДн;

- обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в ПО ИСПДн на стадии его разработки, внедрения и сопровождения;

- может располагать любыми фрагментами информации о ТС обработки и защиты информации в ИСПДн.

8. К восьмой группе относятся персонал, обслуживающий ТС ИСПДн, а также лица, обеспечивающие поставку, сопровождение и ремонт ТС ИСПДн.

Лицо данной группы:

- обладает возможностями внесения закладок в ТС ИСПДн на стадии их разработки, внедрения и сопровождения;

- может располагать фрагментами информации о топологии ИСПДн, автоматизированных рабочих местах, серверах и коммуникационном оборудовании, а также о ТС защиты информации в ИСПДн.

8.2 Предположения о возможностях нарушителя

Для получения исходных данных о ИСПДн нарушитель (как I категории, так и II категории) может осуществлять перехват зашифрованной информации и иных данных, передаваемых по каналам связи сетям общего пользования и (или) сетям международного информационного обмена, а также по локальным сетям ИСПДн.

Любой внутренний нарушитель может иметь физический доступ к линиям связи, системам электропитания и заземления.

Предполагается, что возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны объектов размещения ИСПДн ограничительных факторов, из которых основными являются режимные мероприятия и организационно-технические меры, направленные на:

- предотвращение и пресечение несанкционированных действий;
- подбор и расстановку кадров;
- допуск физических лиц в контролируемую зону и к средства вычислительной техники;
- контроль за порядком проведения работ.

В силу этого внутренний нарушитель не имеет возможности получения специальных знаний о ИСПДн в объеме, необходимом для решения вопросов создания и преодоления средств защиты ПДн, и исключается его возможность по созданию и применению специальных программно-технических средств реализации целенаправленных воздействий данного нарушителя на подлежащие защите объекты и он может осуществлять попытки несанкционированного доступа к ИР с использованием только штатных программно-технических средств ИСПДн без нарушения их целостности.

Возможность сговора внутренних нарушителей между собой, сговора внутреннего нарушителя с персоналом организаций-разработчиков подсистем ИСПДн, а также сговора внутреннего и внешнего нарушителей должна быть исключена применением организационно-технических и кадрово-режимных мер, действующих на объектах размещения ИСПДн [12].

1.4.3 Морфологический анализ

Позволяет нам определить какие морфологические признаки объекта важны для нас с точки зрения решаемой задачи, затем выявить

существенные свойства по каждому признаку и построить многомерные матрицы, в ячейках которых мы получим сочетания этих свойств и можем выявить наиболее актуальные [6].

Таблица 1 – Морфологический анализ

	Целостность	Доступность	Конфиденциальность	Согласованность	Аутентичность
Программный	Программу нельзя изменить, имеет контрольную сумму.	Доступ к программе осуществляется через ЭВМ.	С программами работают только те пользователи, у которых есть доступ.	Программы аттестованы регулятором.	Программа работает без ошибок и артефактов.
Аппаратный	За оборудованием идет контроль со стороны службы безопасности.	К оборудованию допуск у лиц обеспечивающих работоспособность системы.	К аппаратной части (сервера/автоматизированные системы) имеют доступ только сотрудники с допуском.	Непротиворечивость компонентов задействованных в системе.	Качество оборудования соответствует требованиям.
Персонал	Работник выходит из системы по	Доступ по разрешительной системе	Уровни допуска персонала.	Непротиворечивость действий	Достоверность и

	окончанию рабочей сессии.	доступа.		сотрудника с системой и персоналом.	подлинность выполненной им работы.
Обеспечивающий	Правовая база является устойчивой и не подлежит кардинальной изменчивости.	К документам имеется доступ только у доверенных лиц.	Документы хранятся в режимно-секретном помещении.	Документы и правовая база не противоречит друг другу.	Документы описывают проблему с достаточной полнотой.

1.5 Выбор и обоснование методологии решения задачи

1.5.1 Анализ существующих мер по предотвращению рисков ИБ в ИСПДн

Вопросам анализа подходов управления рисками ИБ посвящено большое количество научных трудов, большинство из которых либо изобилуют наличием математических формул и моделей; либо не содержат вообще никаких математических изысков; либо в них существует перевес в сторону какой-либо из двух выше приведенных групп подходов. Проанализируем содержательные аспекты каждой группы подходов [11].

Подходы первой группы, как правило, используют различные разделы высшей математики: теорию множеств, теорию вероятностей, дискретную математику и т.д. В качестве ядра подходов выбирают

принципы, основанные на теории шансов или полезности (надежности), или нечетких множеств, а также непрерывные или дискретные распределения и т.д. Работы, относящиеся к первой группе подходов, зачастую не учитывают реальные требования организаций, занимающихся анализом рисков; требуют от экспертов в области ИБ достаточной математической подготовки; что часто отрицательно сказывается на практике применения данных подходов. Вторая группа подходов в большей степени развита зарубежными авторами. Статьи авторов из США, Англии носят прежде всего рекомендательный характер для модернизации, пересмотра некоторых вещей уже работающих, зарекомендовавших себя стандартов ИБ: ISO, BS, не требующих глубокого знания высшей математики [8].

Третья группа подходов во многих случаях сочетает в себе экспертные оценки и оценки рисков, базирующиеся на определении их вероятности по имеющимся статистическим данным. Подобные подходы можно успешно применять в практической деятельности (не смотря на ряд минусов), так как использование базы статистики позволяет свести к минимуму субъективную точку зрения эксперта на решаемую задачу и проводить работу по оценке рисков ИБ специалистам без большого опыта, квалификации. Далее будут более подробно проанализированы первая и вторая, с учетом стандартов ИБ России, группы подходов к оценке рисков ИБ. В некоторых работах осуществлены подходы, использующие теории графов, нечеткой логики. Это позволяет более наглядно представить причинно-следственные связи между объектами, потоками информационной системы, что, в свою очередь, способствует наиболее точному анализу системы на этапе ее проектирования, облегчает работу экспертов по определению оценок рисков ИБ. Кроме того, анализ рисков осуществляют более формализовано, с более простой программной реализацией. Для подходов второй группы естественно использовать прописи стандартов ИБ, федеральных нормативных

документов, рекомендаций. Хотя им не стоит слепо доверять, но такое решение задач ИБ экономит время работы специалистов по защите информации. Очевидные плюсы применения стандартов безопасности не отражены в большинстве проанализированных подходов. Как будет показано ниже, лишь небольшое количество из них основано, или хотя бы использует, некоторые рекомендации стандартов ИБ. Многие организации до сих пор придерживаются старых способов точечного управления уязвимостями, вместо управления рисками. Такой выбор затрудняет возможную сертификацию организации, требует от специалистов по безопасности освоения, повышения опыта в новых для них системах анализа рисков. Кроме того, работа в рамках способов управления уязвимостями затрудняет эксплуатацию обязательных в настоящий момент рекомендаций, нормативных документов ФСТЭК и ФСБ РФ. Отсюда использовать указанные выше способы лучше не полностью, а выбирать некоторые рекомендации, которые не нарушают работу по анализу рисков, но могут повысить точность итоговых результатов, сократить время работы экспертов. Процесс анализа рисков является составной частью общей системы управления организацией, поэтому для более качественной работы с рисками информационных систем выбирают общую процессную модель. Модель отражает работу стандартного цикла управления Деминга, определяет: Планирование – Выполнение – Проверку – Корректировку. В стандартах ISO и BS присутствует проекция данного процесса на работу по анализу и управлению рисками ИБ. В большинстве рассмотренных нами подходов осуществляют работу чаще всего только по пункту оценки рисков, то есть непосредственно по разделу «Выполнение». Таким образом, подсчет рисков, выполненная на его основе закупка новых средств и разработка подходов по повышению безопасности, ненамного отличается по качеству от применяемого в аварийных ситуациях так называемого «заплаточного» метода. Только полностью осуществленный цикл управления,

последующее его циклическое повторение с корректировкой, пересмотром рисков, позволяет обеспечить ИБ с помощью анализа рисков. Нельзя не заметить отсутствие для ряда обсуждаемых подходов экономической составляющей анализа. В результате получают, что управление рисками – это только закупка средств защиты, без учета возможностей данной организации. Сравнительный анализ: Сравнение подходов проводили по следующим параметрам: субъективные оценки сложности вычисления и программной реализации; способ ввода входных данных в систему анализа; вид итогового результата анализа – вид выходных данных; использование стандартов ИБ. Оценка сложности вычислений представляет собой субъективную характеристику сложности использования рассматриваемых подходов, может принимать значения: «Высокая», «Средняя», «Низкая» сложность. На результат «высокой» оценки наибольшее влияние оказывает применение специальных математических теорий, тогда как решения на основе таблиц, экспертных оценок можно характеризовать низкой сложностью вычислений. Сложность программной реализации также оценивали на основе субъективного мнения. Поэтому, на мой взгляд, можно отметить следующее, что использование математической логики, теории графов облегчает задачу программиста. Далее, входные данные в систему анализа рисков могут поступать несколькими способами. Основные из них: статистические данные, экспертные оценки. Оба вида данных имеют свои плюсы и минусы, могут быть предназначены для работы в различных ситуациях. На Рисунке 6 представлена статистика по использованию того или иного типа ввода данных в рассматриваемых подходах.

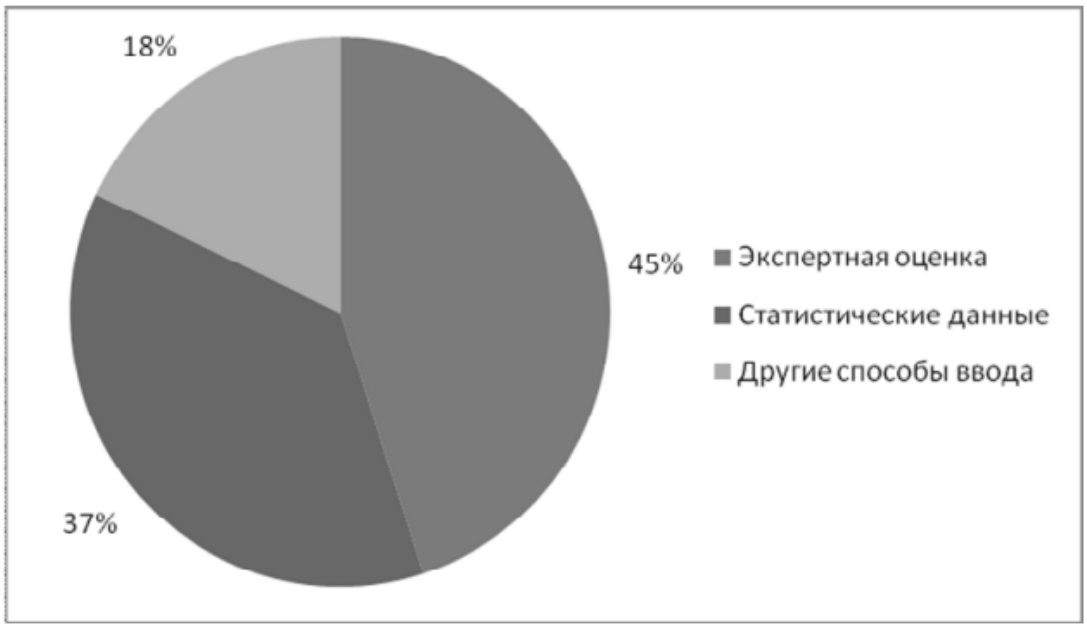

Рисунок 6. Соотношение типов входных данных рассматриваемых подходов

Аналогично входным данным, анализировали типы итоговых результатов. Чаще всего выходные данные представляют в виде количественной или качественной оценки. Хотя количественная оценка является, в большинстве своем, вероятностью риска (точечной оценкой), качественная характеристика более наглядна, дает возможность более простого ранжирования рисков. Статистика типов выходных данных анализируемых подходов представлена на рисунке 7.

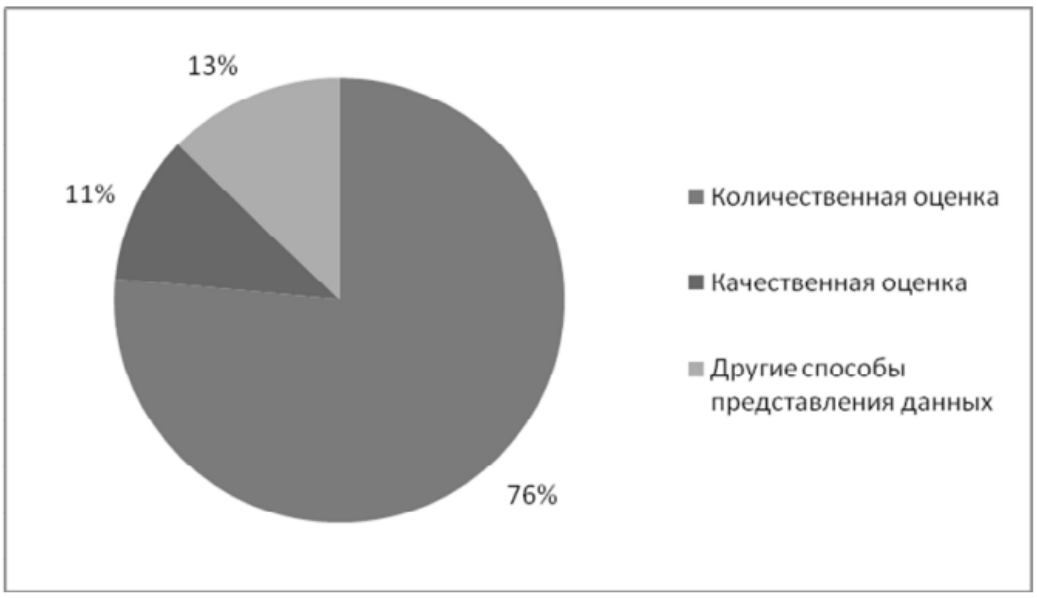

Рисунок 7. Соотношение типов выходных данных рассматриваемых

подходов

Сравнительный анализ существующих методов определения рисков информационной безопасности

Как видно из соотношения, количественная оценка преобладает в подходах, представленных в научных статьях, хотя большинство стандартов безопасности используют качественную шкалу оценки. Последней исследуемой характеристикой сравнения подходов является применение стандартов безопасности, нормативных документов. На Рисунке 8 представлена статистика их использования.

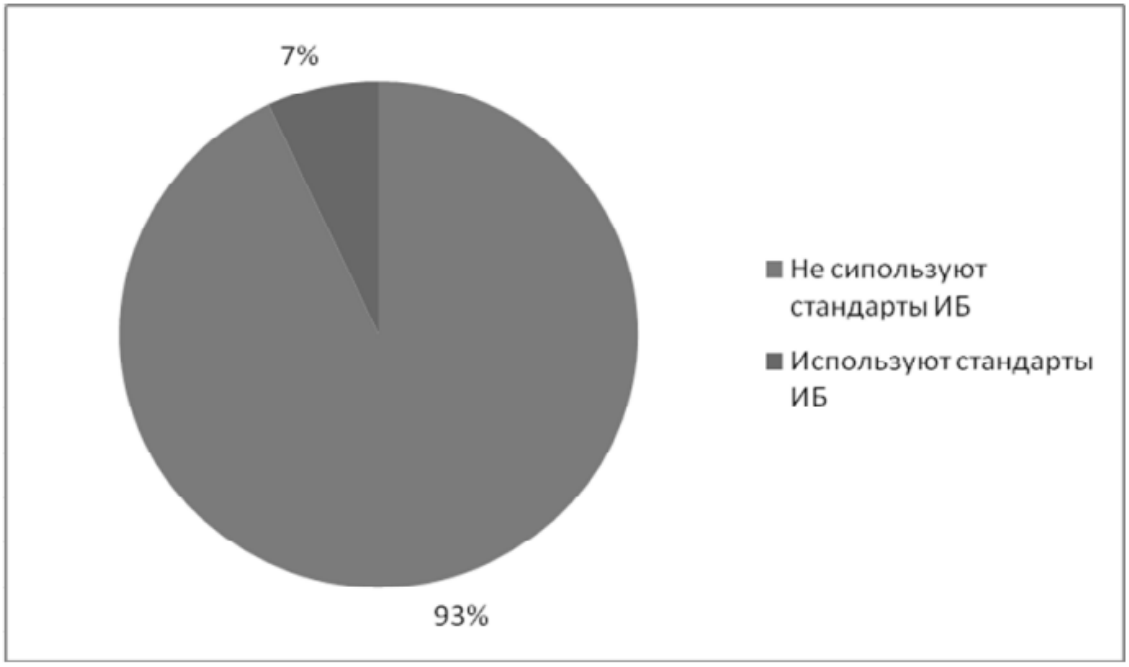

Рисунок 8. Соотношение использования стандартов ИБ и

нормативных границ IP-адресов и подготовиться к следующей эффективной атаке.

Анализ действующей нормативно-правовых документов в области ИБ, на основе регуляторов ФСТЭК России и ФСБ России, позволяют сделать обоснованный вывод об отсутствии единого метода предотвращения рисков нарушения информационной безопасности распределённых информационных системах . Ключевыми ограничениями существующих методологий по формированию модели угроз и предотвращения рисков ИБ являются:

− отсутствие не субъективных и обоснованных методов оценивания;

− рассмотрение объекта атак и угрозы/риска ИБ с точки зрения организации/оператора/владельца или требований нормативных документов, но не с точки зрения нарушителя. С одной стороны, это приводит к недостаточной защищенности и потерям организации, а с другой стороны к не эффективному расходованию ресурсов организации (как финансовых, так и человеческих);

− используются экспертные и численные методы оценки значений параметров, использующихся для вычисления вероятности угроз и рисков ИБ. Известные методики формирования модели угроз и оценки рисков ИБ обеспечивают получение оценок угроз БИ только в конкретный момент времени − «мгновенные» оценки вероятности угроз ИБ и соответствующих рисков для ИС, которые, однако, с неизбежностью изменяются с течением времени. Так как, например, нарушитель, совершивший успешную атаку, будучи необнаруженным, имеет возможность в течение длительного времени собирать информацию о средствах защиты внешнего и внутреннего периметра ИС и готовить следующую результативную атаку.

1.5.2 Методы решения

По результатам анализа сделаны следующие выводы: большинство подходов не учитывают концепции, требования различных стандартов ИБ, что может вызвать недоверие к применяемым подходам у экспертов, проводящих анализ рисков ИБ, затрудняет возможную сертификацию организации. Многие подходы, в основе которых лежит цель получить количественную оценку рисков с использованием математических формул, моделей, углубляясь в математические теории, теряют связь с практической оценкой рисков, реальными бизнес требованиями. Ряд подходов не обеспечивают полного процесса по оценке, управлению рисками ИБ, реализуя лишь некоторые его компоненты. Анализ показывает, что большое количество рассматриваемых подходов

содержат свежие идеи, концепции по проведению оценки рисков [7]. Учитывая сильные и слабые стороны существующих подходов, можно сделать попытку проектирования и реализации более совершенного подхода к управлению рисками ИБ.

Для решения проблемы, связанной с предотвращением рисков нарушений ИБ в распределённых системах обработки персональных данных. Существуют компании, предоставляющие услуги по размещению ИСПДн различного уровня защищенности в подготовленной ими инфраструктуре. Количество таких компаний существенно увеличилось после публикации Федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам осуществления государственного контроля (надзора) и муниципального контроля» от 18.07.2011 №242-ФЗ, обязывающий компании хранить собираемые персональные данные о гражданах Российской Федерации на территории страны.

Но это всё равно не может даёт возможности быть уверенным в том, что данные находятся в безопасности и не подвержены рискам.

Но это всё равно не может даёт возможности быть уверенным в том, что данные находятся в безопасности и не подвержены рискам.

Для достижения поставленной цели в рамках компании «СофтИнформ» будет использоваться классический метод расчёта рисков, представленный в NIST 800-30 [17]:

$$R = P(t) \cdot S, \quad (1)$$

где R – значение риска;

P(t) – вероятность реализации угрозы информационной безопасности (применяется смесь качественной и количественной шкалы);

S – степень влияния угрозы на актив (цена актива в качественной и количественной шкале).

В рассматриваемых методиках, в качестве методических указаний [18], сказано использовать межсетевой экран для предотвращения атак. В данной работе, я буду рассматривать на сколько эти методы остаются актуальными на сегодняшний день.

Для реализации расчета вероятности реализации угрозы информационной безопасности данным методом будут собраны оценки экспертов по информационной безопасности.

Выводы по 1 главе:

В данной главе был проведен анализ распределенной информационной системы, особенности с точки зрения информационной безопасности, а также описаны особенности рассматриваемого объекта.

Построены модели угроз и нарушителя согласно руководящим документам, и проведён морфологический анализ. Также были проанализированы существую методы предотвращения рисков.

Были решены задачи, поставленные для достижения цели:

- Описать особенности организации с точки зрения информационной безопасности.
- Проанализировать текущие методы предотвращения рисков информационной безопасности в информационных системах.

ГЛАВА 2. ПРАВКТИЧЕСКАЯ РЕАЛИЗАЦИЯ МЕТОДОВ УПРАВЛЕНИЯ РИСКАМИ

2.1 Определение наиболее вероятных угроз для выбранной организации

2.1.1 Атака SQL -иньекция

SQL-инъекция, или SQLi, - это уязвимость, которая позволяет злоумышленнику использовать фрагмент вредоносного кода на языке структурированных запросов (SQL) для управления базой данных и доступа к потенциально ценной информации. Атаки, основанные на таких угрозах, являются наиболее распространенными и опасными: они могут быть нацелены на любое веб-приложение или веб-сайт, который взаимодействует с базой данных SQL (подавляющее большинство баз данных реализовано на SQL).

Как происходит атака SQL-инъекцией?

Чтобы понять, как работает SQL-инъекция, вам сначала нужно понять, что такое язык SQL. SQL - это язык запросов, используемый для чтения, изменения и удаления информации, хранящейся в реляционной базе данных. Поскольку большинство веб-сайтов и веб-приложений взаимодействуют с базами данных SQL, атаки с использованием SQL-инъекций могут нанести серьезный ущерб организации.

SQL-запрос - это запрос, отправляемый в базу данных для выполнения определенной операции или функции (например, извлечения данных или выполнения кода SQL). Например, запрос может отправлять учетные данные пользователя через веб-форму для доступа к веб-сайту. Эти веб-формы обычно настроены на прием только определенных типов данных, таких как имена пользователей и/или пароли. Введенная информация будет сопоставлена с базой данных. Если все совпадает, пользователь может войти на веб-сайт. В противном случае в доступе будет отказано.

Эта ситуация опасна, поскольку большинство веб-форм не имеют механизма для предотвращения ввода другой информации в поля. Это

дает злоумышленникам возможность отправлять свои собственные запросы в базу данных через поля ввода формы. Они могут использовать эту уязвимость для различных преступных целей, от кражи конфиденциальных данных до манипулирования информацией в базах данных.

Поскольку подавляющее большинство веб-сайтов и серверов используют базы данных, SQL-инъекция является одним из старейших и наиболее распространенных видов кибератак. В сообществе киберпреступников есть несколько инцидентов, которые увеличивают вероятность таких атак: во-первых, мы говорим об инструментах, которые могут помочь вам обнаружить уязвимости SQL-инъекций. Соответствующие утилиты предоставляются бесплатно в виде проектов с открытым исходным кодом. Просто нажмите нужную кнопку, и в течение нескольких минут будет запущен ata-ka, который позволит вам получить доступ к любой таблице или столбцу в базе данных.

Симптомы атаки SQLI

Успешная атака с использованием SQL-инъекции может никоим образом не произойти. Однако иногда вы можете заметить следующие симптомы:

- Получено слишком много запросов за короткий промежуток времени. Например, поток электронной почты из формы обратной связи на веб-сайте.

-Рекламные блоки, которые перенаправляют пользователей на определенные веб-сайты.

-Странные всплывающие окна и сообщения об ошибках.

Типы SQL-инъекций

В зависимости от того, как осуществляется доступ к внутренним данным сервера и как это может повлиять на реализацию SQL, их можно разделить на три категории:

Внутриполосная атака (внутриполосный SQLi)

Это самый простой тип атаки для злоумышленника, поскольку для завершения атаки и получения результата используется один и тот же канал связи. Этот тип атаки SQLi делится на две подкатегории:

-Атаки, основанные на ошибках (SQLi основан на ошибках). При этом типе атаки действия злоумышленника могут привести к тому, что база данных будет генерировать сообщения об ошибках. Основываясь на полученном сообщении об ошибке, злоумышленник попытался разобраться в инфраструктуре базы данных.

-Атаки на основе альянса (SQLi основан на альянсе). Злоумышленник получает необходимые данные, используя оператор SQL UNION для объединения нескольких инструкций SELECT в один HTTP-ответ.

Вывод SQLi, также известный как слепая SQL-инъекция

При этом типе атаки злоумышленник изучает реакцию и поведение сервера после отправки записи, чтобы узнать больше о структуре базы данных. В этом случае никакие записи из базы данных веб-сайта не будут отправлены злоумышленнику, и он не увидит их в том же канале связи во время внутренней атаки (отсюда и название "слепая SQL-инъекция"). Эта атака делится на два подтипа:

-Слепая атака, основанная на времени (SQLi основана на времени). Злоумышленник отправляет SQL-запрос в базу данных, заставляя ее ждать несколько секунд, прежде чем подтвердить или отклонить полученный запрос.

-Логическая слепая атака (логическое значение SQLi). Злоумышленник отправляет SQL-запрос в базу данных и ожидает ответа "да" или "нет".

Атаки за пределами полосы SQLi

Эта атака происходит в двух ситуациях:

- Когда злоумышленник не может выполнить атаку и собрать данные по тому же каналу связи, или

-Если сервер работает слишком медленно или нестабильно, он не достигнет желаемого эффекта [9].

2.1.2 Атака сканирование сети

Цель этой атаки - выяснить, какие компьютеры подключены к сети и какие сетевые службы на ней запущены.

Первая задача решается с помощью утилиты ping для отправки эхо-сигналов ICMP и обхода всех сетевых адресов по очереди или редактирования эхо-сигналов на широковещательные адреса.

Попытки сканирования могут быть определены путем анализа трафика и отслеживания эхо-сигналов, отправленных полным узлом за короткий промежуток времени. Чтобы предотвратить обнаружение, злоумышленник может продлить время отправки сообщения. Вы можете использовать сегмент TCP с кодом из первой цифры вместо эхо-сообщения в качестве ответа на несуществующий DNS-запрос. Если злоумышленник получает в ответ недоступный целевой пакет ICMP с кодом 1 (хост недоступен), тестируемый хост не работает или не подключен к сети [15].

Чтобы определить, какие службы запущены, вам необходимо знать, какие порты открыты, поскольку некоторые службы назначены определенным портам (TCP-портам). Затем эта информация может быть использована для запуска атак более высокого уровня. Существует несколько способов сканирования TCP-портов. Самый простой способ - установить TCP-соединение с тестовым портом. В этом случае будет большое количество открытых и незакрытых подключений, поэтому атаки в этой реализации будут легко обнаружены. Другим методом является так называемое полуоткрытое сканирование. В этом режиме злоумышленник передает сегмент сообщения (кодовый бит которого равен SYN) на тестовый порт и ожидает ответа. Если в качестве ответа получен сегмент, содержащий первый фрагмент кода, это означает, что порт закрыт, а если получен сегмент, содержащий фрагменты кода SYN

и ACK, это означает, что порт открыт. Затем злоумышленник отправляет пакет с первым флагом на порт [16]. Это масштабирование труднее обнаружить, поскольку соединение еще не было открыто.

Другой вариант - отправить сегмент с флагом FIN (больше никаких данных от отправителя), PSH (функция push), URG (поле аварийного указателя имеет значение) или даже пустое поле с кодом. Если порт закрыт, ответом является сегмент с первым флагом, если ответа нет, порт открыт (поскольку эти сегменты просто игнорируются).

2.2 Определение векторов атаки

Наиболее подходящий вектор для развития атак "Сканирование сети" и « SQL injection » является - " Сбор информации о сетевой инфраструктуре " [4]. Так как именно этот подход к реализации угроз дает наиболее полное представление о сети организации, что в свою очередь позволяет хакерам точнее задействовать свои инструменты и добиваться поставленного результата, путем проведения дальнейших действий с сетевой инфраструктурой организации.

Вектор атак сбор информации о сетевой инфраструктуре был выбран исходя из приказа федеральной службы по техническому и экспортному контролю [18], так как они реализуются с набольшей вероятностью в данной системе. Вектор атак будет направлен на отдел экономики и финансов.

2.3 Подготовка среды исследования

Для проведения исследования будет разработан стенд, который будет моделировать отдел экономики и финансов. Этот отдел был выбран не случайно, в нём присутствует сервер баз данных в котором присутствует информация о сотрудниках организации, финансовых операциях компании, информация об организациях подряда. Данный отдел взаимодействует со сторонними организациями, государственными органами, путём переписки через электронную почту, а также через официальные ресурсы государственной власти.

Модель отдела будет реализована при помощи программы VMware Workstation 16 Pro , это программное обеспечение для виртуализации операционных систем на основе Windows и Linux , в нем есть возможность виртуализировать как 32 разрядные, так и 64 разрядные операционные системы, есть возможность запускать несколько виртуальных машин одновременно и объединять в общую сеть.

За основу операционных систем отдела экономики и финансов будут взяты ОС Windows 7, эти системы наиболее распространены в этой сфере, а также наиболее понятны и не требующих глубоких познаний для пользователя.

Для проведения исследования были построены 3 виртуальные машины, в настройках виртаульных машин был создан новый виртуальный интерфейс, че рез который компьютеры подключаются к виртуальному свитчу. Затем машинам были присвоены адреса одной подсети и для проверки пропингованы между собой, данные действия представлены на рисунках 9-12.

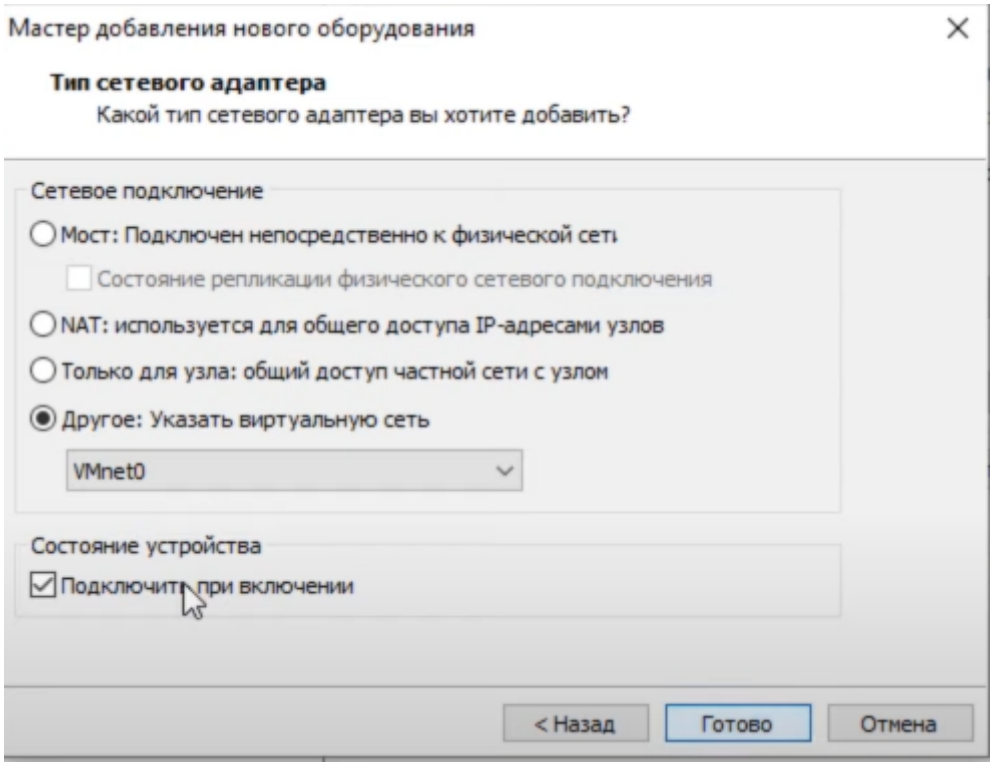

Рисунок 9. Создание виртуального интерфейса

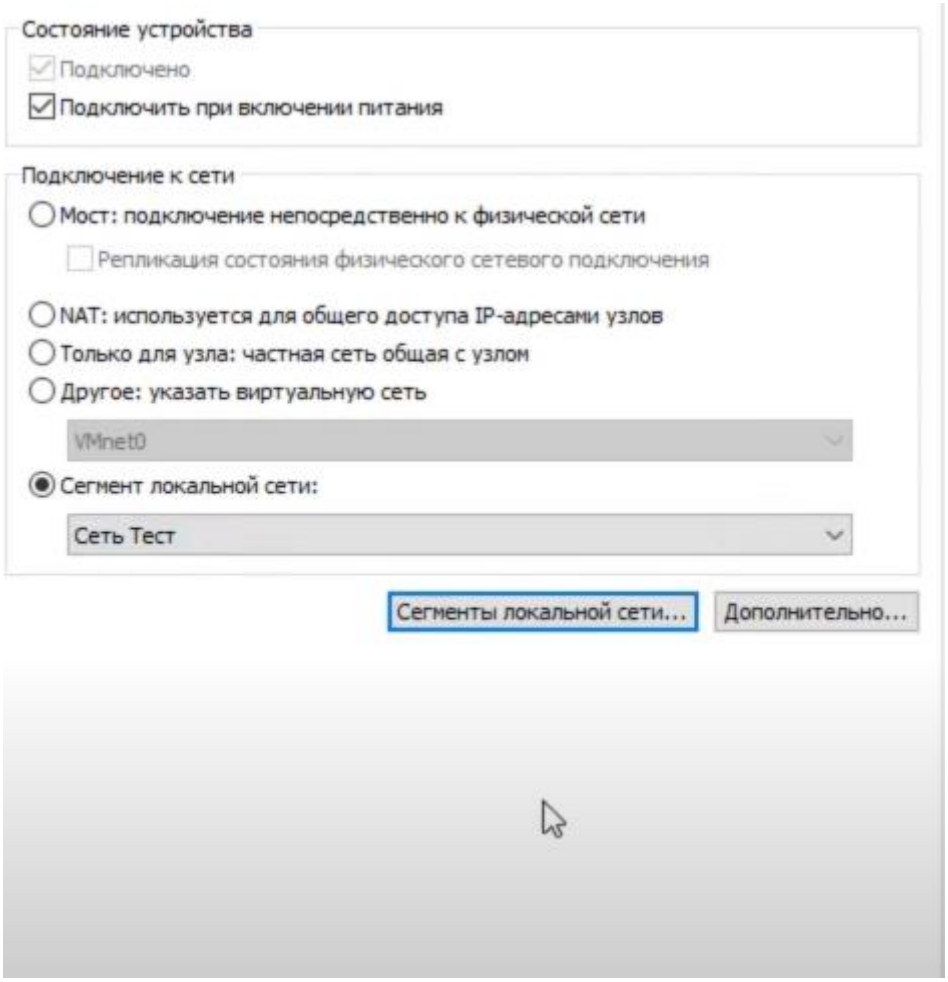

Рисунок 10. Создание виртуального свитча

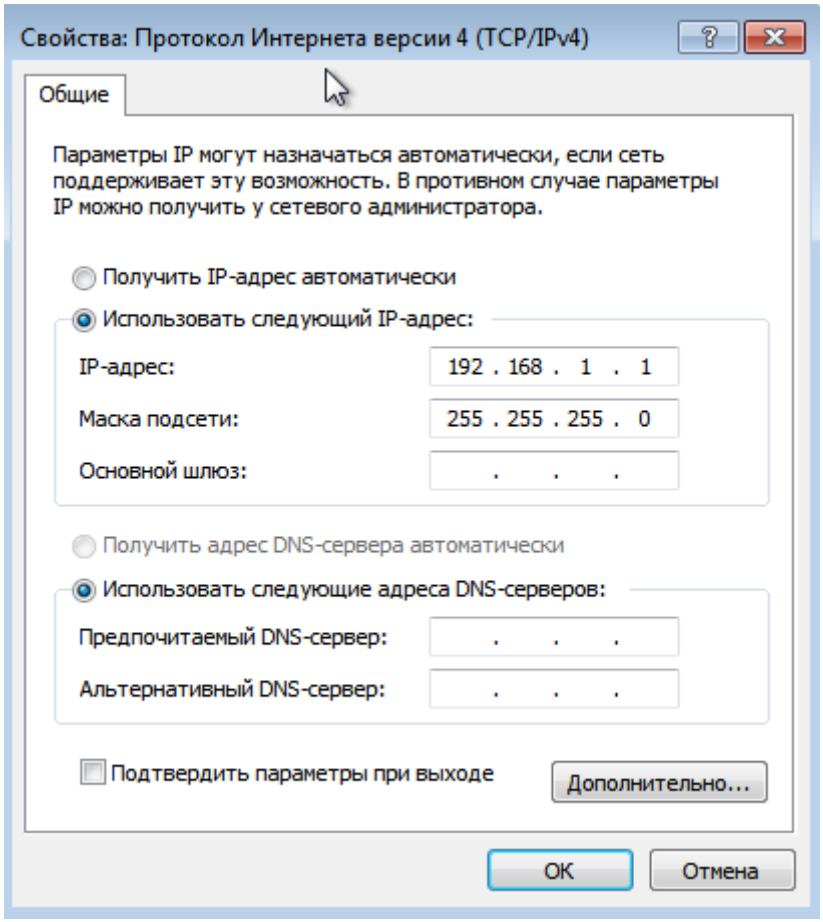

Рисунок 11. Присвоение ip адресов

```
C:\Users\James>ping 192.168.1.1

Обмен пакетами с 192.168.1.1 по с 32 байтами данных:
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=64
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=64
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=64
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=64

Статистика Ping для 192.168.1.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
```

Рисунок 12. Проверка пингом

2.4 Реализация исследования

Для реализации атак по заданному вектору в первом случае были использованы такие инструменты как: Maltega , SQL injection .

Чтобы получить исходные данные, для успешного совершения атаки посредством инструмента SQL injection была просканирована сеть организации «СофтИнформ» при помощи Maltega , начиная с известного

узла, находящегося в открытой сети интернет, что позволило получить больше данных о топологии сети, представленной на рисунке 13.

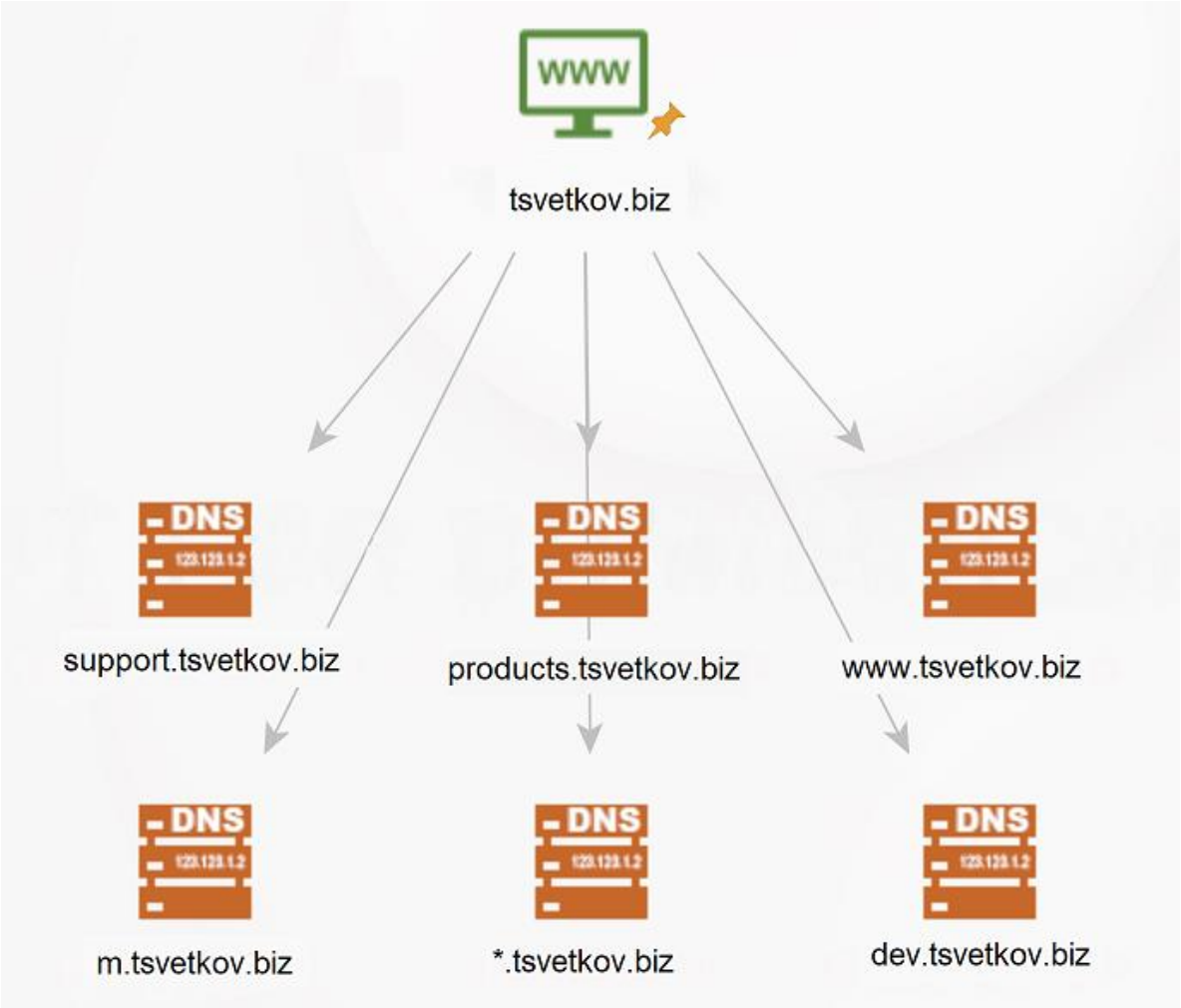

Рисунок 13. Топология сети

Далее, анализируя полученные данные, было выявлено, что сайт, который хостится на сервере, так же имеет связь с сервером, принимающим персональные данные пользователей. Эта информация позволила определить объект на который будет производиться атака.

Затем через инструмент SQL injection проводим атаку на сайт, рисунок 14.

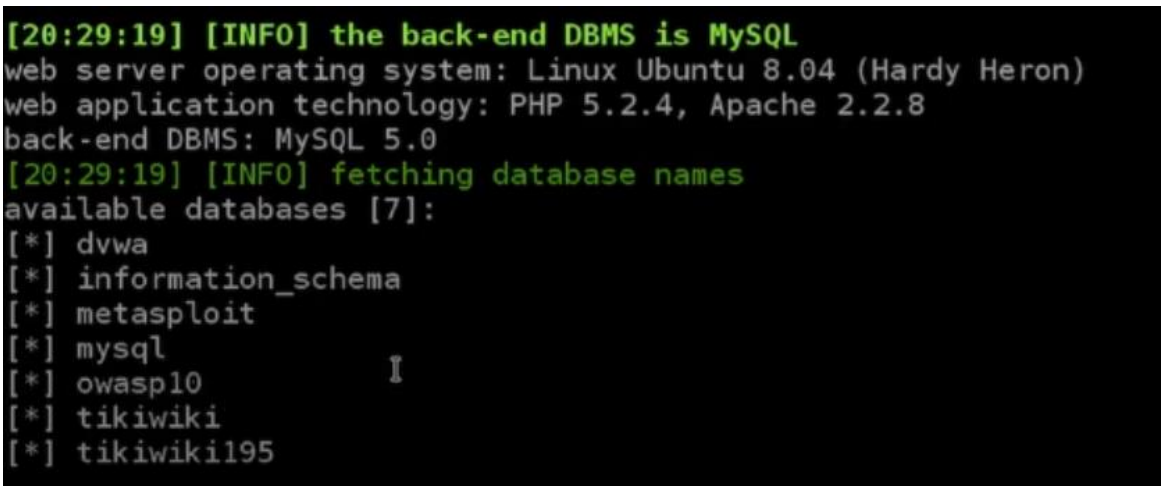

Рисунок 14. Список баз данных сайта

После этого выбираем интересующую нас базу данных и скачиваем нужные нам столбцы, рисунок 15-16.

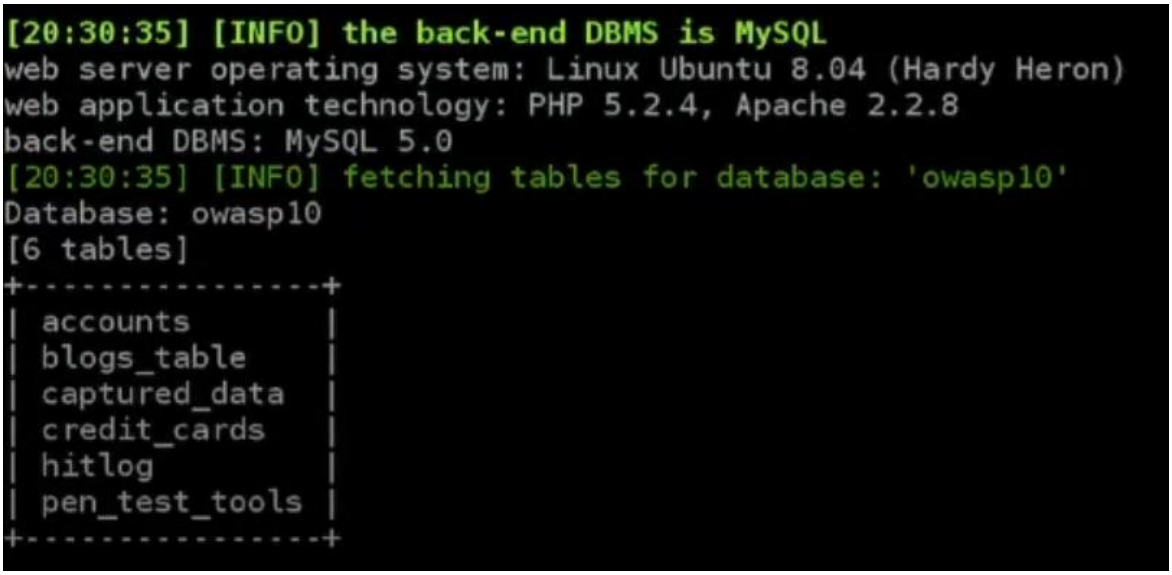

Рисунок 15. Столбцы базы данных owasp 10

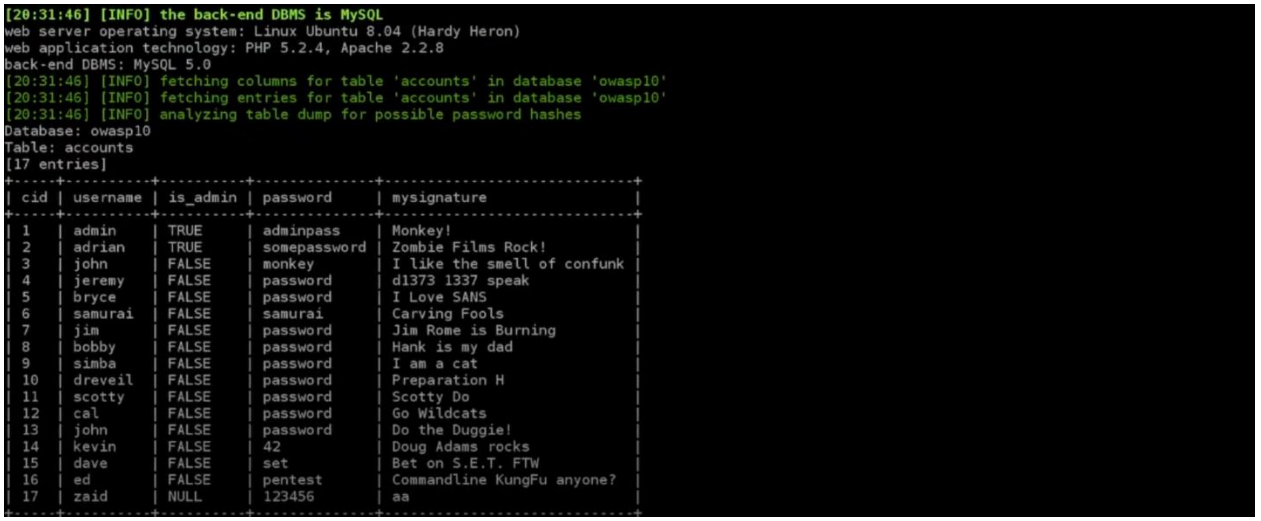

Рисунок 16. Значения в столбцах accounts

На данном этапе считаю, что атака SQL -инъекция реализована, доступ к сведениям, содержащим персональные данные получен.

Чтобы предотвратить эту атаку, есть несколько вариантов:

- Используйте автоматизированные инструменты для поиска SQL-инъекций.

- Защита базы данных на уровне кода.

- Используйте белый список. Белый список - для обозначения действительных ключей и значений.

- Используйте PDO . Используя PDO и заполнители, можно значительно снизить риск внедрения, поскольку данные и запросы отправляются отдельно. Сначала устанавливается соединение с базой данных, затем подготавливается запрос, затем индивидуально указываются переменные и, наконец, выполняется запрос.

- Проверить происхождение данных - Недостаточно обработать данные - нужно выяснить происхождение данных.

- Манипулирование переменными - попробуйте экранировать кавычки, заменить служебные символы, удалить лишние пробелы и т. д.

- Не используйте метод GET в формах - передача переменных таким способом очень опасна, так как они видны пользователю. Если информация важна, лучше использовать POST. По ссылке злоумышленник может не только узнать имя переменной, но и какое значение она должна иметь — так он сможет выбрать лучшую переменную для внедрения.

В дальнейшем проведена атака на сайт с уже защитными мерами в качестве сетевого экрана (WAF), с названием VipNet Office Firewall, в результате чего информации из баз данных получить не удалось.

Далее для реализации атаки сканирование сети будет использоваться инструмент Nmap .

Nmap является свободно распространяемой, бесплатной утилитой, которая служит хорошим инструментом для гибкого сканирования сетей.

Он выступает отличной альтернативой аналогичным инструментам, благодаря своей гибкости и относительной простоты настройки сканируемых параметров. Так же его можно отметить из-за большого сообщества и множества инструкций, которые может изучить как человек с атакующей стороны - хакер, так и специалист по информационной безопасности.

Для выполнения сканирования, ранее был получен Ip адрес сайта организации из открытых источников, на него и будет осуществляться сканирование, рисунок 17

```
root@papacarlo-virtual-machine:~# nmap -v 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2023-01-25 21:43 MSK
Initiating ARP Ping Scan at 21:43
Scanning 192.168.1.1 [1 port]
Completed ARP Ping Scan at 21:43, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:43
Completed Parallel DNS resolution of 1 host. at 21:43, 0.01s elapsed
Initiating SYN Stealth Scan at 21:43
Scanning 192.168.1.1 [1000 ports]
Discovered open port 139/tcp on 192.168.1.1
Discovered open port 554/tcp on 192.168.1.1
Discovered open port 445/tcp on 192.168.1.1
Discovered open port 135/tcp on 192.168.1.1
Discovered open port 49153/tcp on 192.168.1.1
Discovered open port 49154/tcp on 192.168.1.1
Discovered open port 49156/tcp on 192.168.1.1
Discovered open port 10243/tcp on 192.168.1.1
Discovered open port 49155/tcp on 192.168.1.1
Discovered open port 2869/tcp on 192.168.1.1
Discovered open port 5357/tcp on 192.168.1.1
Discovered open port 49152/tcp on 192.168.1.1
Completed SYN Stealth Scan at 21:43, 4.76s elapsed (1000 total ports)
Nmap scan report for 192.168.1.1
Host is up (0.00022s latency).
Not shown: 988 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 00:0C:29:4C:70:B5 (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.89 seconds
           Raw packets sent: 1990 (87.544KB) | Rcvd: 14 (600B)
```

Рисунок 17. Сканирование портов при помощи Nmap

Как можем наблюдать, атака сканирование сети проведена успешно, данные о портах получены и могут использоваться для проведения дальнейших атак.

В дальнейшем была проведена атака на этот же адрес, но уже с установленным межсетевым экраном VipNet Office Firewall , который сертифицирован по 4-му классу защищённости, рисунок 18.

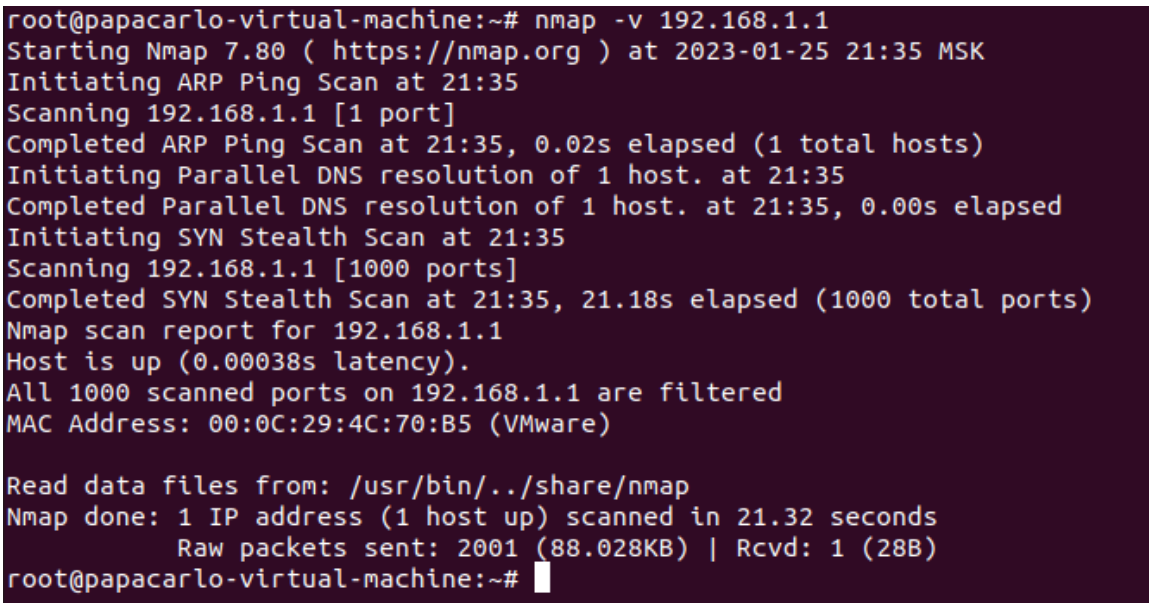

Рисунок 18. Атака на закрытые порты

В результате атаки можем увидеть, что никакой информации о портах получить не удалось.

Вывод по 2 главе:

В данной главе были определены наиболее вероятные угрозы для рассматриваемой системы, а также определены основные векторы атак. Был подготовлен стенд и смоделировано поведение системы в определённых условиях.

Проверено соответствие методических указаний в современном информационном пространстве.

Были решены задачи, поставленные для достижения цели :

- Проанализировать текущие методы предотвращения рисков информационной безопасности в информационных системах

- Подготовить стенд для моделирования угроз на рассматриваемую систему

- Смоделировать поведение системы, при воздействии выбранных атак

ГЛАВА 3. РАСЧЁТЫ И АНАЛИЗ РЕЗУЛЬАТОВ

3.1 Сбор информации для анализа

Для расчётов значения рисков R , необходимо иметь значения P(t) – вероятности реализации угрозы информационной безопасности, в связи с этим был проведен опрос экспертов информационной безопасности. В качестве экспертов были выбраны специалисты по защите информационной безопасности организации АО "НПП "Радар ммс". Эксперты выбирались по таким критериям как:

- опыт в сфере информационной безопасности не менее 3 лет;
- возраст от 27 до 55 лет;

В опросе приняло участие 10 экспертов, подходящие под критерии.

Всем экспертам был задан вопрос:

- Как вы оцениваете вероятность реализации угроз сканирование сети и сбор информации о сетевой инфраструктуре описанной организации.

Таблица 2 – Определение вероятности реализации угрозы информационной безопасности, до проведения исследования на стенде

Номер эксперта	Возраст эксперта (лет)	Опыт в сфере информационной безопасности (лет)	Оценка вероятности реализации угрозы сбор информации о сетевой инфраструктуре	Оценка вероятности реализации угрозы сканирование сети
1	32	8	0,15	0,25
2	43	15	0,35	0,35
3		10	0,50	0,50

	42			
4	28	3	0,05	0,15
5	53	16	0,25	0,35
6	29	4	0,40	0,45
7	31	11	0,30	0,25
8	44	12	0,35	0,10
9	42	6	0,20	0,30
10	51	23	0,35	0,40

Результаты были записаны успешно получены, затем этим же экспертам был задан следующий вопрос:

- Как вы оцениваете вероятность реализации угроз сканирование сети и сбор информации о сетевой инфраструктуре описанной организации, если данная сетевая структура была построена на стенде, а угрозы успешно реализованы.

Таблица 3 – Определение вероятности реализации угрозы информационной безопасности, после реализации угроз на стенде.

Номер эксперта	Возраст эксперта (лет)	Опыт в сфере информационной безопасности (лет)	Оценка вероятности реализации сбор информации о	Оценка вероятности реализации угрозы сканирование

			сетевой инфраструктуре	сети
1	32	8	0,60	0,65
2	43	15	0,50	0,55
3	42	10	0,50	0,60
4	28	3	0,55	0,30
5	53	16	0,45	0,60
6	29	4	0,70	0,50
7	31	11	0,60	0,70
8	44	12	0,65	0,70
9	42	6	1	1
10	51	23	0,50	0,50

Следующим вопрос для экспертов был:

- Как вы оцениваете вероятность реализации угроз сканирование сети и сбор информации о сетевой инфраструктуре описанной организации, если данная сетевая структура была построена на стенде, а также установлен межсетевой экран VipNet Office F ir ewall , который успешно предотвратил реализацию рассматриваемых угроз.

Таблица 4 – Определение вероятности реализации угрозы информационной безопасности, после успешного предотвращения угроз на стенде.

Номер эксперта	Возраст эксперта (лет)	Опыт в сфере информационной безопасности (лет)	Оценка вероятности реализации угрозы сбор информации о сетевой инфраструктуре	Оценка вероятности реализации угрозы сканирование сети
1	32	8	0,05	0,15
2	43	15	0,10	0,10
3	42	10	0,25	0,25
4	28	3	0,15	0,10
5	53	16	0,10	0,20
6	29	4	0,35	0,15
7	31	11	0,30	0,10
8	44	12	0,05	0,10
9	42	6	0,10	0,15
		23	0,20	0,20

10	51			

3.2 Расчёт результатов

В результате проведенного опроса среди специалистов по информационной безопасности с разным возрастом и опытом работы, мы получили данные для обработки представленные в таблицах 1 и 2. Проводя разбор генеральной выборки, для получения значения P(t) – вероятности реализации угрозы информационной безопасности, необходимо провести расчёты для получения среднего значения вероятности сбор информации о сетевой инфраструктуре:

$$P(t) = \frac{0,15+0,35+0,50+0,05+0,25+0,40+0,30+0,35+0,20+0,35}{10} = 0,29$$

Аналогичным способом рассчитываем значение для угрозы сканирование сети:

$$P(t) = \frac{0,25+0,35+0,50+0,15+0,35+0,45+0,25+0,10+0,30+0,40}{10} = 0,31$$

Таким мы получили значения вероятности реализации угрозы, а также имеем значения активов организации, представленные в первой главе и теперь можем рассчитать риски по формуле (1).

Значения активов из первой части работы:

- Оборудование – оценочная стоимость 75000000 рублей
- Денежные средства – 57000000 рублей
- Рыночные ценные бумаги 25000000 рублей
- Здания, сооружения – оценочная стоимость 185000000 рублей
- Торговые марки – оценочная стоимость 20000000 рублей
- Программные продукты – оценочная стоимость 60000000 рублей

Теперь рассчитываем риск для угрозы сбор информации о сетевой инфраструктуре:

R=0,29*75000000=21750000 рублей

R=0,29*57000000=16530000 рублей

R=0,29*25000000=7250000 рублей

R=0,29*185000000=53650000 рублей

R=0,29*20000000=5800000 рублей

R=0,29*60000000=17400000 рублей

Далее по такому же принципу рассчитываем риски для угрозы сканирование сети:

R=0,31*75000000=23250000 рублей

R=0,31*57000000=17670000 рублей

R=0,31*25000000=7750000 рублей

R=0,31*185000000=57350000 рублей

R=0,31*20000000=6200000 рублей

R=0,31*60000000=18600000 рублей

Следующим этапом проводим расчёты для получения среднего значения вероятности реализованной на стенде угрозы сбор информации о сетевой инфраструктуре таким же способом, что представлен выше:

$$P(t) = \frac{0,60+0,50+0,50+0,55+0,45+0,70+0,60+0,65+1+0,50}{10} = 0,60$$

Затем рассчитываем среднее значение вероятности для реализованной на стенде угрозы сканирование сети:

$$P(t) = \frac{0,65+0,55+0,60+0,30+0,60+0,50+0,70+0,70+1+0,50}{10} = 0,61$$

Далее рассчитываем риски для реализованной на стенде угрозы сбор информации о сетевой инфраструктуре:

R=0,60*75000000=45000000 рублей

R=0,60*57000000=34200000 рублей

R=0,60*25000000=15000000 рублей

R=0,60*185000000=111000000 рублей

R=0,60*20000000=12000000 рублей

R=0,60*60000000=36000000 рублей

И риски для реализованной на стенде угрозы сканирование сети:

R=0,61*75000000=45750000 рублей

R=0,61*57000000=34770000 рублей

R=0,61*25000000=15250000 рублей

R=0,61*185000000=112850000 рублей

R=0,61*20000000=12200000 рублей

R=0,61*60000000=36600000 рублей

Теперь сравним полученные значения рисков до реализации атак и успешно реализованных атак на стенде.

Для угрозы сбор информации о сетевой инфраструктуре:

21750000 рублей < 4500000 рублей

16530000 рублей < 34200000 рублей

7250000 рублей < 15000000 рублей

53650000 рублей < 111000000 рублей

5800000 рублей < 12000000 рублей

17400000 рублей < 36000000 рублей

И для угрозы сканирование сети:

23250000 рублей < 45750000 рублей

17670000 рублей < 34770000 рублей

7750000 рублей < 15250000 рублей

57350000 рублей < 112850000 рублей

6200000 рублей < 12200000 рублей

18600000 рублей < 36600000 рублей

Подводя промежуточные итоги можем отметить, что при успешной реализации атак на стенде, оценки вероятности экспертов увеличились, соответственно увеличились и риски, что мы и наблюдаем при сравнении результатов.

Следующим этапом проводим аналогичные расчёты для получения среднего значения вероятности, успешно предотвращенной на стенде атаки сбор информации о сетевой инфраструктуре:

$$P(t) = \frac{0,05+0,10+0,25+0,15+0,10+0,35+0,30+0,05+0,10+0,20}{10} = 0,16$$

Также рассчитываем среднее значение вероятности для успешно предотвращённой на стенде угрозы сканирование сети:

$$P(t) = \frac{0,15+0,10+0,25+0,10+0,20+0,15+0,10+0,10+0,15+0,20}{10} = 0,15$$

И рассчитываем риски для успешно предотвращенных на стенде угрозы сбор информации о сетевой инфраструктуре:

R=0,16*75000000=12000000 рублей

R=0,16*57000000=9120000 рублей

R=0,16*25000000=4000000 рублей

R=0,16*185000000=29600000 рублей

R=0,16*20000000=3200000 рублей

R=0,16*60000000=9600000 рублей

Далее считаем риски для успешно предотвращенных на стенде угрозы сканирование сети:

R=0,15*75000000=11250000 рублей

R=0,15*57000000=8550000 рублей

R=0,15*25000000=3750000 рублей

R=0,15*185000000=27750000 рублей

R=0,15*20000000=3000000 рублей

R=0,15*60000000=9000000 рублей

После проведения всех расчётов, сравниваем полученные вначале значения до реализации угроз и после успешного предотвращения угроз.

Для угрозы сбор информации о сетевой инфраструктуре:

21750000 рублей > 12000000 рублей

16530000 рублей > 9120000 рублей

7250000 рублей > 4000000 рублей

53650000 рублей > 29600000 рублей

5800000 рублей > 3200000 рублей

17400000 рублей > 9600000 рублей

Для угрозы сканирование сети:

23250000 рублей > 11250000 рублей

17670000 рублей > 8550000 рублей

7750000 рублей > 3750000 рублей

57350000 рублей > 27750000 рублей

6200000 рублей > 3000000 рублей

18600000 рублей > 9000000 рублей

Цена же межсетевого экрана VipNet Office Firewall составляет 100000 рублей, что несопоставимо с потерями, которые может понести компания, не используя данный метод защиты.

3.3 Анализ полученных результатов

В результате проведенных опросов можем наблюдать, как меняются вероятности реализации угрозы информационной безопасности, определяемая экспертами в сфере информационной безопасности. Зная, что та или иная система будет предотвращать угрозы информационной безопасности или же наоборот будет открыта к реализации атак.

В данном случае видим, что после успешной реализации атак SQL-инъекция и сетевое сканирование, риски возросли достаточно значительно относительно начальных значений для каждого риска.

После проведения этих же атак на уже защищённую систему межсетевым экраном VipNet Office Firewall, может увидеть, что атаки успешно предотвращены и оценки вероятности реализации угроз, определяемые экспертами, значительно снизились. Если посмотреть на расчёты, можем увидеть, что соответственно вероятности, снизились и риски, что и является главной целью текущей работы.

Представленные в методике требования остаются актуальными и на сегодняшний день. Такое требование как установленный межсетевой экран

является неотъемлемой частью для обеспечения безопасности системы обработки персональных данных.

Выводы по 3 главе:

В данной главе был проведен сбор информации для анализа рисков информационной безопасности, а также произведён их расчёт. Были проанализированы полученные результаты.

Решенные задачи, поставленные для достижения цели:

- Опросить экспертов в сфере информационной безопасности для получения статистических данных
- Произвести расчёты и анализ полученных результатов
- Проверка предлагаемых методиками средств защиты

ЗАКЛЮЧЕНИЕ

В дипломной работе была рассмотрена распределенная информационная система на примере компании «СофтИнформ», в перечень деятельности которой входит обработка персональных данных.

В результате работы был проведен анализ методических документов и существующих работ по предотвращению рисков, а также описание системы, в том числе и с точки зрения защиты информации. Построены модели угроз и нарушителей, согласно регламентирующим документам регулирующих органов.

Были определены наиболее вероятные угрозы для выбранной организации и определены вектора атак для этих угроз. Затем был подготовлен стенд, для моделирования атак и анализ поведения системы в результате этих атак. В ходе следования требованиям методики за 2013 год.

На следующем этапе был проведён сбор информации у экспертов по информационной безопасности и проведен расчёт рисков для рассматриваемой системы. Затем все результаты проанализированы.

В результате цель работы, а именно - снизить риски информационной безопасности распределенной информационной системы, была достигнута.

Поставленные в начале работы задачи, для достижения цели, а именно:

Задачи поставленные для достижения цели:

- Описать особенности организации с точки зрения информационной безопасности

- Проанализировать текущие методы предотвращения рисков информационной безопасности в информационных системах

- Подготовить стенд для моделирования угроз на рассматриваемую систему

- Смоделировать поведение системы, при воздействии выбранных атак

- Опросить экспертов в сфере информационной безопасности для получения статистических данных

- Произвести расчёты и анализ полученных результатов

- Проверка предлагаемых методиками средств защиты

Были успешно выполнены.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1.Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801 (Дата обращения 08.09.2022)

2.Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]. Режим доступа: https://fstec.ru/component/attachments/download/289 (Дата обращения 25.09.2022)

3.Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]. Режим доступа: https://fstec.ru/component/attachments/download/290 (Дата обращения 17.12.2022)

4.Описание векторов компьютерных атак [Электронный ресурс]. Режим доступа: https://b4.cooksy.ru/articles/opisaniya-vektorov-kompyuternyh-atak-soderzhaschihsya-v-bazah-dannyh (Дата обращения 12.12.2022)

5.Бурлов В.Г. Математические методы моделирования в экономике. Часть 1. СПб: изд-во СПбГПУ, 2007. - 330 с (Дата обращения 10.12.2022)

6.Выбор наиболее опасных уязвимостей для перспективных информационных систем критического применения [Электронный ресурс]. Режим доступа: https://cyberrus.com/wp-content/uploads/2022/01/66-75-147-22_7.-Gryzunov.ПДННf (Дата обращения 09.01.2023)

7.Методический документ. Методика оценки угроз безопасности информации [Электронный ресурс]. Режим доступа: https://fstec.ru/en/component/attachments/download/2919 Дата обращения 09.01.2023)

8. Методика оценки угроз безопасности информации

[Электронный ресурс]. Режим доступа: https://www.evraas.ru/resources/metodika-otsenki-ugroz-bezopasnosti-informatsii/ (Дата обращения 21.01.2023)
9.Что такое SQL-инъекция? Определение и описание [Электронный ресурс]. Режим доступа: https://www.kaspersky.ru/resource-center/definitions/sql-injection (Дата обращения 08.01.2023)
10. Анализ пользовательских данных с целью использования его результатов в коммерческих целях [Электронный ресурс]. Режим доступа: https://elar.urfu.ru/bitstream/10995/54390/1/m_th_s.n.lubarsky_2017.ПДННf (Дата обращения 09.01.2023)
11. Сравнительный анализ существующих методов определения рисков информационной безопасности [Электронный ресурс]. Режим доступа: http://elib.altstu.ru/journals/Files/pv2011_03_01/ПДННf/221pletnov.ПДННf (Дата обращения 10.01.2023)
12. Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в информационных системах персональных данных ОГПОБУ «технический колледж» [Электронный ресурс]. Режим доступа: http://texkolobl.ru/IT/model_ugroz.ПДННf (Дата обращения 12.10.2022)
13.Угрозы безопасности персональных данных в учреждении [Электронный ресурс]. Режим доступа: https://www.elibrary.ru/download/elibrary_23681535_43983132.ПДННf (Дата обращения 12.12.2022)
14. Классификация угроз и уязвимостей информационной безопасности в корпоративных системах [Электронный ресурс]. Режим доступа: https://www.elibrary.ru/download/elibrary_20289801_23234078.ПДННf (Дата обращения 16.01.2023)
15. Атаки на сеть. Часть 2 [Электронный ресурс]. Режим доступа: https://habr.com/ru/company/otus/blog/659417/ (Дата обращения 16.01.2023)
16. Сканирование сети [Электронный ресурс]. Режим доступа: https://dic.academic.ru/dic.nsf/ruwiki/1333843 (Дата обращения 03.01.2023)

17. Risk Management Guide for Information Technology Systems [Электронный ресурс]. Режим доступа: https://csrc.nist.gov/publications/detail/sp/800-30/archive/2002-07-01 (Дата обращения 03.01.2023)
18. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ПРИКАЗ от 18 февраля 2013 г. N 21 [Электронный ресурс]. Режим доступа: https://fstec.ru/component/attachments/download/561 (Дата обращения 20.11.2022)