Тип работы: Дипломная работа

Предмет: Информационные технологии

Содержание

Введение 3
Глава 1. Анализ общих требований к обеспечению защиты информации в автоматизированных системах предприятий 5
1.1 Общие требования к защищенности вычислительных сетей 5
1.2 Характеристика видов угроз и моделей нарушителей 7
1.3 Основные задачи обеспечения защиты информации в локальных сетях 17
2. Общая характеристика объекта защиты 28
2.1. Общая характеристика МЭШ 28
2.2. Общая характеристика сетевой инфраструктуры образовательного учреждения 30
2.3. Общая характеристика системы сетевой защиты в условиях МЭШ 37
3. Проектирование системы шифрования канала связи в условиях МЭШ 41
3.1. Использование технологии VPN для обеспечения передачи данных 41
3.2.Технико-экономическое обоснование 51
Заключение 56
Список использованных источников 58
Приложение 61

Введение

Актуальность
Специфика работы образовательных учреждений такова, что в соответствии с технологией работы необходимо осуществление обмена информацией, доступ к которой является ограниченными в соответствии с требованиями законодательства.
Таким образом, для обеспечения нужного уровня защищенности необходимо создать защищённую сетевую инфраструктуру, обеспечивающую защиту от несанкционированного доступа.
Обеспечение защиты персональных данных в настоящее время является актуальной задачей в силу того, что утечка данных, позволяющих идентифицировать личность людей, может привести к негативным последствиям для субъекта персональных данных, что включает: потерю имущества, предоставление несанкционированного доступа к банковским счетам, обнародованию конфиденциальной информации и др.
Это связано с тем, что с внедрением систем электронного документооборота становится возможным предоставление доступа к аккаунтам субъекта по предъявлению определенного типа персональной информации.
Политика информационной безопасности должна предусматривать комплекс мероприятий, связанных с обеспечением организационных мер, разработкой документационного обеспечения защиты информации, разработкой регламентов использования программной защиты информации, физической защиты помещений, а также защиты от утечек информации с использованием каналов связи.
Обеспечение защиты персональных данных в настоящее время регламентировано в различных законодательных актах федерального уровня, а также отраслевых документах. Таким образом, при использовании информационных систем, в которых проводится обработка персональных данных необходимо принятие мер по обеспечению их защищенности в соответствии с установленными стандартами.
Цель этой работы заключается в разработке анализе системы удаленного доступа с использованием VPN в условиях МЭШ.
Задачи работы:

- анализ теоретических аспектов обеспечения сетевой безопасности;
- анализ видов защищаемой информации в условиях образовательного учреждения;
- выбор программных решений для шифрования каналов связи;
- технико-экономическое обоснование проекта.
Объект исследования: информационная система МЭШ
Предмет исследования: система защиты канала передачи данных в условиях МЭШ.

Глава 1. Анализ общих требований к обеспечению защиты информации в автоматизированных системах предприятий

1.1 Общие требования к защищенности вычислительных сетей

Обеспечение безопасности информационных ресурсов от сетевых атак связано с принятием мер по обеспечению защиты от утечек данных и защиты работоспособности системы от угроз, связанных с активностью удаленных сетевых узлов. Основными целями сетевых атак являются: нарушение конфиденциальности хранящихся сведений на уделённых системах, а также нарушение их работоспособности.
Существует несколько принципов классификации сетевых атак.
Первый вид классификации - по принципу воздействия. Задачей пассивных сетевых атак является получение несанкционированного доступа к защищаемым информационным ресурсам, находящимся на удаленных серверах. Примерами пассивных сетевых атак являются: получение доступа к ящикам электронной почты, закрытым частям сайтов. Методы атак в данном случае связаны с подбором паролей и сертификатов. Обеспечение защиты от атак указанного типа связано с усложнением парольной защиты, обеспечением конфиденциальности хранилища сертификатов, блокированием доступа к системе при определении признаков проведения атаки.
При проведении активных сетевых атак целью является не только чтение данных, но и их изменение. Классифицировать сетевые атаки можно также в соответствии с задачами, поставленными атакующей системой (например, в качестве цели может рассматриваться не только получение доступа к информации, но также формирование бот-сети, а также нарушение функциональности сервера).
Ряд сетевых атак может быть связан с отправкой большого количества запросов на удаленные системы, в результате которых нарушается их работоспособность.
В настоящее время проводится разработка и совершенствование методов защиты от сетевых атак, однако полноценной гарантии от проведения успешной атаки ни один из методов дать не может. Дело в том, что любая статичная система защиты имеет недостатки, и задача защиты от всех сетевых атак является невозможной. Динамические методы защиты, использующие статистические алгоритмы, экспертные системы, модули обеспечения защиты, системы на основе нечеткой логики и нейронных сетей, обладают множеством недостатков, в силу того, что базируются на алгоритмах анализа подозрительной активности с проведением ее сопоставления с известными алгоритмами сетевых атак. Таким образом, неизвестные типы атак могут обходить установленные системы защиты.
Таким образом, любая современная информационная система должна обладать системой защиты от сетевых атак, исключающей возможности утечки и модификации данных. Если данная система связана с технологиями жизнеобеспечения, то необходимо проведение сертификации системы на предмет защиты от внешних уязвимостей.
Так, основными методами защиты от сетевых атак являются:
- шифрование каналов связи;
- использование систем комплексной защиты информации;
- использование ПО для защиты от сетевых атак;
- проведение оптимальных настроек защиты средствами сетевой операционной системы.
Компоненты защиты информации от сетевых атак включают в себя:
- организационную составляющую (издание ряда нормативных документов, регламентирующих вопросы защиты информации, обучение пользователей технологиям защиты от сетевых атак, распознаванию их признаков, действиям при обнаружении признаков атаки);
- программную составляющую в части установки и настройки специального программного обеспечения для защиты от сетевых атак с возможностью централизованного управления системой;
- инженерно-техническую составляющую в целях предотвращения физического проникновения

злоумышленников на объекты, а также предотвращения утечек сетевой информации по каналам различной физической природы.
Построение архитектуры защиты от сетевых атак должно производиться в соответствии с утвержденными стандартами и соответствующей моделью угроз и моделью нарушителя. Класс защищенности системы, в соответствии с которым проектируется архитектура защиты информации, присваивается по результатам аудита системы защиты информации, который проводится сторонними сертифицированными организациями, либо специалистами самой организации, имеющими соответствующие компетенции.
Далее проведем анализ основных технологий защиты от сетевых атак в условиях МЭШ.
1.2 Характеристика видов угроз и моделей нарушителей

Проведем анализ основных типов угроз сетевой безопасности.
Одним из критериев классификации сетевых угроз является их происхождение, в данном случае угрозы безопасности делятся на угрозы, связанные с влиянием человеческого фактора и угрозы, связанные с особенностями работы аппаратного обеспечения.
Угрозами технического характера являются [10]:
- ошибки в работе программного обеспечения;
- проведение внешних DoS- и DDoS-атак;
- действие вредоносного программного обеспечения;
- осуществление несанкционированного съема информации;
- активность сетевых угроз.
Алгоритм DDoS-атаки показан на рисунке 1.

Рисунок 1 - Алгоритм проведения DDoS-атаки

Источниками уязвимостей в системном и прикладном программном обеспечении являются:
- программные закладки, представляющий собой скрытый функционал, открывающий возможности проведения сетевых атак на объект, на котором развернуто ПО;
- ошибки в системах безопасности, возникающие в случаях, когда разработчики неумышленно пренебрегают обеспечением защищенности программной системы.
DoS - и DDoS-атаки
Denial Of Service (получение отказа в обслуживании) - особый тип атак, которые направлены на выведение ресурсов сети или серверов из режима нормального функционирования. При проведении DDOS-атак наблюдается генерация трафика, приводящая к отказу в обслуживании вследствие достижения объемов передачи данных предельного значения пропускной способности сети, либо вычислительной мощности сервера. Результатам DDOS-атаки является невозможность обслуживания запросов на сервер, остановка работы Web-сервисов. Например, в случае банковских систем или серверов государственных органов, последствия могут быть связаны с остановкой технологических процессов и, как следствие, значительными материальными потерями.
Угрозы вредоносного программного обеспечения.
Одной из наиболее распространённых категорий опасностей в рамках функционирования информационных систем является вредоносное программное обеспечение, в качестве источника могут выступать: почтовые программы, прикладное ПО, заражения посредством внешних носителей информации.
Активность вредоносных программных систем может проявляться в нарушении функциональности компьютера, похищении конфиденциальной информации, создании на основе зараженных компьютеров бот-сетей, используемых для проведения атак. Также широкое распространение имеют программы-шифровальщики.
Работа анализаторов протоколов и «снифферов»
К данной группе относятся средства по перехвату передаваемых по сети данных, включая активные сетевые атаки. Указанные средства могут представлять собой как аппаратные, так и программные решения. Как правило, передача данных осуществляется по сети в открытой форме, что дает возможность злоумышленникам внутри локальной сети осуществлять их перехват. В некоторых сетевых протоколах (POPS, FTP) не используется механизм шифрования паролей, что дает возможность злоумышленникам перехватывать и использовать их по своему усмотрению. При передаче информации по глобальным сетям данная проблема является наиболее острой. По возможности необходимо ограничивать доступ к ресурсам сети неавторизированным пользователям.

Рассмотрим механизм использования технических средств съема информации.
К устройствам подобного рода относятся различные виды клавиатурных жучков, мини-камер, звукозаписывающих устройств и т.д. Указанная группа используется в повседневной жизни намного реже вышеперечисленных, так как, кроме наличия специальной техники, требует доступа к сети и ее компонентам.
Далее рассмотрим виды угроз, обусловленных влиянием человеческого фактора. К угрозам данного типа можно отнести:
- уволенных или недовольных сотрудников;
- технологии промышленного шпионажа;
- угрозы, связанные с халатностью сотрудников;
- угрозы, обусловленные недостаточной квалификацией сотрудников.
Уволенные и недовольные сотрудники
Данная группа людей является наиболее опасной, так как многие из работающих сотрудников могут иметь разрешенный доступ к ресурсам локальной сети предприятия. Особое внимание в данном случае следует обратить на системных администраторов, знакомых с архитектурой сетевой безопасности системы и имеющих возможности реализации несанкционированного доступа к ней.
Одним из наиболее распространённых источников уязвимостей в информационных системах является пренебрежение сотрудниками требованиями информационной безопасности. Как правило, в организациях существуют утвержденные инструкции, описывающие порядок безопасного использования ресурсов Интернета, электронной почты, использования внешних носителей информации, мобильных устройств. Соблюдение данных правил в некоторой степени может замедлять выполнение технологических процессов. Многие сотрудники для того, чтобы ускорить выполнение рабочих операций, склонны обходить ограничения информационной безопасности, что потенциально может приводить к негативным последствиям для защищенности информационных ресурсов.
Так, примерами халатности в отношении средств защиты информации могут быть:
- несоблюдение требований к сложности паролей и периодичности их смены;
- передача паролей третьим лицам;
- отключение антивирусной защиты и дополнительных средств защиты информации;
- несоблюдение требований к работе с электронной подписью (например, осуществление входа в браузерное приложение и долговременное отсутствие на рабочем месте, что создает угрозу получения доступа к электронной подписи со стороны злоумышленника);
- отключение защищенных параметров браузера.
Мерами защиты от угроз халатности сотрудников могут быть:
- максимальное понижение уровня доступа пользователя на рабочей станции;
- регламентация временных параметров работы неактивных сеансов;
- принятие нормативных документов и определение ответственности пользователей за нарушение регламентов информационной безопасности.
Низкая квалификация
Зачастую вследствие низкой квалификации пользователю затруднительно понять, с чем он имеет дело; из-за этого даже программные продукты с достаточной степенью защищённости предполагают необходимость тонкой настройки со стороны администраторов безопасности.
Таким образом, защитой от угроз, обусловленных недостаточностью квалификации персонала, могут быть:
- проведение технических учеб со специалистами по вопросам информационной безопасности;
- включение вопросов по информационной безопасности при аттестации сотрудников;
- оценка квалификации сотрудника при принятии на работу или кадровом перемещении.
Таким образом, виды угроз для объектов защиты могут быть разнообразными. Далее приведены примеры некоторых видов угроз, каждой из которых сопоставляются технологические решения, подкрепленные документационным обеспечением (таблица 1):
Таблица 1 - Типовые угрозы безопасности информации

Список использованных источников

1. IDS – Snort. О программе. [Электронный ресурс]. Режим доступа: http://www.netconfig.ru/ready/snort/
2. Сетевая защита информации. [Электронный ресурс]. Режим доступа: http://ic-dv.ru/uslugi/sredstva_doverennoj_zagruzki/

3. Сетевые атаки и их виды. [Электронный ресурс]. режим доступа: https://www.kakprosto.ru/kak-848505-chto-takoe-setevaya-ataka
4. Сетевые атаки и их виды. [Электронный ресурс]. режим доступа: https://www.kakprosto.ru/kak-848505-chto-takoe-setevaya-ataka
5. Гофман М.В. Безопасность сетей ЭВМ : учебное пособие / М.В. Гофман. - Санкт-Петербург: ФГБОУ ВО ПГУПС, 2017. – 241с.
6. Бехроуз А. Криптография и безопасность сетей: учебное пособие / Фороузан А. Бехроуз. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. - 782 с.
7. Новикова Е. Л. Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи: учебник / Е. Л. Новикова. - Москва : Академия, 2018. – 189 с.
8. Новиков С. Н. Методология защиты информации на основе технологий сетевого уровня мультисервисных сетей связи / Новиков Сергей Николаевич. - Новосибирск, 2016. - 39 с.
9. Олифер В. Г., Олифер Н. А. Безопасность компьютерных сетей: [учебный курс] / В.Г. Олифер, Н.А. Олифер. - Москва : Горячая линия - Телеком, 2016. - 643 с.
10. Басыня Е. А. Сетевая информационная безопасность и анонимизация: учебное пособие / Е. А. Басыня. - Новосибирск : Изд-во НГТУ, 2016. – 74с.
11. Лавров Д. Н., Колмаков А. В. Анализ безопасности компьютерных сетей: тесты на проникновение и поиск уязвимостей сетевых протоколов: учебное пособие / Д.Н. Лавров, А.В. Колмаков. - Омск : Изд-во Омского государственного университета, 2016. – 546с.
12. Голиков А.М. Основы проектирования защищенных телекоммуникационных систем [Электронный ресурс]: учебное пособие / А.М. Голиков. - Томск: Томский государственный университет систем управления и радиоэлектроники, 2016. - 396 с
13. Сафонов В.О. Основы современных операционных систем [Электронный ресурс] : учебное пособие / В.О. Сафонов. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. - 826 с
14. Бондарев В. В. Анализ защищенности и мониторинг компьютерных сетей : методы и средства : учебное пособие / В.В. Бондарев. - Москва: Изд-во МГТУ им. Н.Э. Баумана, 2017. – 225с.
15. Михалевич Е.В. Обработка персональных данных: анализ законодательства и судебной практики / Е.В. Михалевич. - Москва : ФГБУ "Редакция "Российской газеты", 2019. - 143 с.
16. Такатлы Д. А. Защита персональных данных / Д. А. Такатлы. - Петропавловск-Камчатский: Дальневосточный филиал Федерального государственного бюджетного образовательного учреждения высшего образования "Всероссийская академия внешней торговли Министерства экономического развития Российской Федерации", 2016. - 92 с.
17. Овчинникова Т. А. Ответственность за нарушение требований законодательства РФ о персональных данных: монография / Т. А. Овчинникова . - Хабаровск : Изд-во ТОГУ, 2018. – 81с.
18. Благодаров А. В. Алгоритмы категорирования персональных данных для систем автоматизированного проектирования баз данных информационных систем / А. В. Благодаров, В.С. Зияутдинов, П.А. Корнев, В.Н. Малыш. - Москва: Горячая линия-Телеком, 2015. - 115 с.
19. Аникин Д. В. Информационная безопасность и защита информации : учебное пособие / Д.В. Аникин. - Барнаул : Изд-во Алтайского государственного университета, 2018. - 196 с.
20. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации / Е. К. Баранова, А. В. Бабаш. - Москва: РИОР ИНФРА-М, 2018. – 334 с.
21. Белобородова Н. А. Информационная безопасность и защита информации: учебное пособие / Н. А. Белобородова. - Ухта : УГТУ, 2016. - 69 с.
22. Горев А. И., Симаков А. А. Обработка и защита информации в компьютерных системах : учебно-практическое пособие / А. И. Горев, А. А. Симаков. - Омск : ОмА МВД России, 2016. - 87 с.
23. Каратунова Н. Г. Защита информации. Курс лекций. - Краснодар: КСЭИ, 2014. - 188 с.
24. Кондратьев А. В. Техническая защита информации. Практика работ по оценке основных каналов утечки : [учебное пособие] / А. В. Кондратьев. - Москва: Горячая линия - Телеком, 2016. - 304 с.
25. Королев Е. Н. Администрирование операционных систем: учебное пособие / Е. Н. Королев. - Воронеж: Воронежский государственный технический университет, 2017. - 85 с.
26. Михайлова Е. М., Анурьева М. С. Организационная защита информации [Электронный ресурс]/ Михайлова Е. М., Анурьева М. С. - Тамбов: ФГБОУ ВО "Тамбовский государственный университет имени Г. Р. Державина", 2017.
27. Никифоров С. Н. Защита информации : защита от внешних вторжений : учебное пособие / С.Н. Никифоров. - Санкт-Петербург: Санкт-Петербургский государственный архитектурно-строительный

университет, 2017. - 82 с
28. Никифоров С. Н. Защита информации: учебное пособие / С.Н. Никифоров. - Санкт-Петербург : СПбГАСУ, 2017. - 76 с.