

Слайд 1

Здравствуйте, уважаемые члены аттестационной комиссии!

Тема моей выпускной квалификационной работы – **«Организация защиты информации от преднамеренных угроз в ЛВС под управлением Windows в ООО «Художественная керамика»».**

Слайд 2

Целью работы является разработка защищенной локальной сети, для повышения уровня сетевой безопасности сети, а также увеличение защищенности имеющихся сегментов сети.

Задачи исследования представлены на слайде.

Слайд 3

Итак, проведенное исследование показало, что политика информационной безопасности и в соответствии с ней построенная система управления информационной безопасностью будет являться наиболее правильным и эффективным способом добиться минимизации рисков нарушения информационной безопасности для локальной сети. Необходимо учитывать, что с течением времени меняется характер угроз, поэтому следует своевременно, используя данные мониторинга и аудита, обновлять модели угроз и нарушителя.

Таким образом, ставится задача разработки модели угроз и модели нарушителя информационной безопасности, основываясь на специфике деятельности данной организации и обеспечивая соответствие государственным стандартам и нормам в области информационной безопасности. Модель угроз информации содержит перечень угроз информации при ее обработке в информационной системе и локальной сети, в частности. В Модели угроз дается описание: информационной системы как объекта защиты, с учетом ее назначения и условий функционирования, состава и категории обрабатываемой защищаемой информации, актуальных источников угроз безопасности информации, потенциального нарушителя безопасности информации.

Угрозы безопасности информации локальной сети, могут дополняться и уточняться по мере выявления новых угроз, появления средств и способов реализации угроз безопасности, изменения требований законодательства в области защиты информации. Модель угроз возможно пересмотреть в будущем по решению руководства или рекомендации уполномоченных органов государственной власти на основе проводимых мероприятий по контролю выполнения требований по обеспечению информационной

безопасности. Состав технических средств и программного обеспечения представлен в таблице.

Слайд 4

Далее на основе анализа условий создания и использования ЗИ определена информация, соответствующая процессам создания и использования ЗИ, которая также может быть объектом угроз.

Слайд 5

Также защищаемую информацию можно сгруппировать по объектам доступа на программном и аппаратном уровнях.

Слайд 6

Итак, основными характеристиками безопасности являются конфиденциальность, целостность и доступность. Характеристики безопасности программного обеспечения локальной сети представлены на слайде.

Слайд 7

Далее на слайде предоставлены характеристики безопасности технических средств локальной сети.

Слайд 8

Итак, нарушение характеристик безопасности ТС может привести к нарушениям характеристик безопасности ПО, ЗИ и СИ, обрабатываемой на данном ТС или с его помощью. Нарушение характеристик безопасности ПО может привести к нарушению доступности ЗИ и СИ, обрабатываемой при помощи данного ПО. Соотношение ТС, ПО, ЗИ и СИ представлено в таблице. Данные таблицы созданы и упорядочены опираясь на базовую модель угроз ФСТЭК. Таким образом, угроза безопасности объекта в нашем случае — это возможное нарушение характеристики безопасности объекта.

Слайд 9

После сбора всей необходимой информации, необходимо определить при помощи каких программных или программно-аппаратных средств будет осуществляться защищенное взаимодействие между офисами, а также внутри каждой из них. Для решения поставленной задачи проводился сравнительный анализ компаний и их предлагаемых ими продуктов. Для этого было отобрано две компании, предоставляющие средства, наиболее подходящие для решения поставленной задачи, это компании ИнфоТеКС и Код

безопасности. Сравнительная таблица приведена на слайде. Так как по условию необходимо создать защищенную локальную сеть для большой сети клиник, сравниваться будут 2 продукта это комплекс VipNet CUSTOM и АПКШ «Континент». Таким образом, на основании проведенного анализа, для создания защищенной сети более удачным является комплекс VipNet CUSTOM, так как он позволяет создавать защищенный канал до самого рабочего места, в то время как другой продукт имеет такую возможность только для удаленного пользователя.

Слайд 10

Итак, перейдем к разработке защищенной локальной сети. В соответствии с рисунком первой сетью будет являться большая сеть главного офиса, в которой существуют различные сегменты, и требуется использование каскадной схемы установки координаторов.

Слайд 11

Далее в соответствии с рисунком второй сетью будут являться удаленные офисы, расположенные в соседнем здании.

Слайд 12

И, наконец, в соответствии с рисунком третьей - филиалы, расположенные в другом городе.

Слайд 13

Таким образом, на рисунке приведена структура с организацией межсетевого взаимодействия, все три сети являются доверенными.

Затем были проведены расчеты, которые показали, что разработка проекта экономически целесообразна для организации. Разработанная система защиты информации от преднамеренных угроз в ЛВС оправдывает себя через полгода.

Слайд 14

Таким образом, в данной работе были даны следующие рекомендации по защите локальной сети:

- требуется защита информационного обмена при прохождении через открытый Интернет;
- требуется, чтобы защищенный туннель был прозрачен для пользователей, которые работают с ресурсами удаленных локальных сетей;

- требуется, чтобы пользователи локальной сети не имели доступа к ресурсам открытого Интернета, за исключением ресурсов других локальных сетей, определенных администратором, с которыми организуется защищенное взаимодействие и, возможно, ресурсов мобильных пользователей;
- требуется исключить необходимость установки ПО ViPNet [Координатор] на шлюзы локальной сети.

Для обеспечения защиты данной локальной сети, достаточно установить программное обеспечение ViPNet. В результате получаем, что он:

- туннелирует открытый информационный обмен между компьютерами удаленных локальных сетей в защищенное соединение от ViPNet данной локальной сети до ViPNet [Координатора] удаленной локальной сети;
- туннелирует открытый информационный обмен между компьютерами своей локальной сети в защищенное соединение от ViPNet [Координатора] данной ЛВС до защищенного мобильного пользователя с программным обеспечением ViPNet [Клиент];
- разграничивает доступ удаленных туннелируемых компьютеров и защищенных мобильных пользователей к ресурсам «своей» локальной сети;
- разграничивает доступ «своих» туннелируемых компьютеров к ресурсам удаленной локальной сети и защищенных мобильных пользователей;
- является сервером IP-адресов, то есть является справочным бюро, которое сообщает защищенным мобильным пользователям о текущем состоянии других объектов VPN и их IP-адресах;
- является сервером для рассылки обновлений;
- является сервером-маршрутизатором для рассылки почтовых сообщений и файлов, посылаемых по «файловому обмену» между объектами VPN;
- является Межсетевым Экраном, который запрещает несанкционированный доступ в локальной сети из Интернета.

Так же, мы рассмотрели основные угрозы на данную не защищенную автоматизированную систему и программное обеспечение ViPNet, что позволило нам построить защиту этой автоматизированной системы. Проделав этот анализ можно сказать, что предъявленные требования по защите автоматизированной системы были выполнены, и организована защита канала между несколькими локальными сетями через Internet, а так же организованы туннели на однокарточных Координаторах.

Слайд 15

Таким образом, Цель работы достигнута.

Спасибо за внимание! Доклад окончен.