МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ Федеральное государственное автономное образовательное учреждение высшего образования «СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению лабораторных работ
по дисциплине
ПРОГРАММНО-АППАРАТНЫЕ КОМПЛЕКСЫ ЗАЩИТЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Направление подготовки	**10.03.01 Информационная безопасность**
Профиль	Комплексная защита объектов информатизации
Квалификация выпускника	бакалавр
Форма обучения	очная
Учебный план	2020 г.

Пятигорск, 2020 г.

СОДЕРЖАНИЕ

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью изучения дисциплины является формирование у студентов знаний и умений по защите компьютерной информации с применением современных программно-аппаратных средств; содействие развитию системного мышления.

Задачами дисциплины являются:

- Дать основы о методах и средствах защиты информации в компьютерных системах;
- Дать основы правил разграничения доступа и основных функций СЗИ, его обеспечивающих;
- Дать основы практических аспектов построения систем ограничения доступа и других СЗИ;
- Дать основы аппаратной реализации различных средств защиты информации;
- Дать основы о защитных механизмах, реализованных в средствах защиты компьютерных систем от несанкционированного доступа (НСД);
- Дать основы вопросов защиты ПО от несанкционированного использования;
- Дать основы о применении средств криптографической защиты информации и средств защиты от НСД для решения задач обеспечения информационной безопасности;
- Дать основы методов защиты от РПВ;
- Дать основы методов и особенностей защиты объектов ОС;
- Дать основы принципов построения файловой системы и моделей разграничения доступа к объектам.

Приобретенные знания и навыки позволят студентам работать в должностях администраторов компьютерных сетей и администраторов безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Программно-аппаратные комплексы защиты объектов информатизации» относится к базовой части блока дисциплин Б1ОП ВО подготовки бакалавра направления 10.03.01 «Информационная безопасность». Ее освоение происходит в 7семестре.

3. СВЯЗЬ С ПРЕДШЕСТВУЮЩИМИ ДИСЦИПЛИНАМИ

При изучении данной дисциплины необходимы знания, полученные в результате освоения дисциплин «Программно-аппаратные средства защиты информации», «Техническая защита информации».

4. СВЯЗЬ С ПОСЛЕДУЮЩИМИ ДИСЦИПЛИНАМИ

Знания, полученные при изучении данной дисциплины, необходимы для защиты выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

5. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Код	Формулировка:
ОК-5	способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты

	интересов личности, общества и государства, соблюдать нормы профессиональной этики
ОПК-4	способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации
ПК-1	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
ПСК-2	способностью применять современные информационные технологии и методы цифровой обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем

6. НАИМЕНОВАНИЕ ЛАБОРАТОРНЫХ РАБОТ

№ темы	Наименование тем дисциплины, их краткое содержание	Обьем часов	Интерактивная форма проведения
	7 семестр		
4	Лабораторная работа №1. Принципы защиты файрволом типа 3+ (Kerio PF)	1,5	Компьютерные
4	Лабораторная работа №2. Принципы построения VPN сети (VipNet)	3	
4	Лабораторная работа №3. Принципы защиты отдельных сервисов с помощью туннелирования трафика (ZeBeDee)	3	
4	Лабораторная работа №4. Система защиты корпоративной информации «Secret Disk»	3	
5	Лабораторная работа №5. Использование протокола IPSec для защиты сетей	3	
5	Лабораторная работа № 6. Организация VPN средствами СЗИ StrongNet	3	Компьютерные симуляции
6	Лабораторная работа № 7. Принципы защиты программно-аппаратным комплексом SecretNet	3	Компьютерные симуляции
7	Лабораторная работа № 8. Принципы защиты программно-аппаратным комплексом Dallas Lock	3	Компьютерные симуляции
8	Лабораторная работа №9. Освоение принципов документального оформления структуры и работы защищенных (Digital Security Office)	4,5	
	Итого	27	10,5

7. СОДЕРЖАНИЕ ЛАБОРАТОРНЫХ РАБОТ

Лабораторная работа № 1
«Принципы защиты файрволом типа 3+ (Kerio PF)»

Форма проведения: лабораторная работа.

Цель работы:

Ознакомиться с принципами защиты файрволом типа 3+ (Kerio PF) в компьютерных системах.

Процесс подключения корпоративной информационной системы к Интернету связан с решением двух основных задач. Первая из них — предоставить контролируемый совместный доступ сотрудников к глобальной сети. Вторая же — обеспечить защиту от внешних угроз. Часто их рассматривают и решают отдельно друг от друга с помощью разных инструментов.

Однако такой подход имеет целый ряд недостатков. В частности , повышенные затраты на внедрение и обслуживание такой системы. Гораздо удобнее использовать комплексные продукты, которые, с одной стороны обеспечивают совместную работу в Интернете, а с другой — надежно защищают сеть от всего спектра внешних угроз. В качестве примера можно взять Kerio WinRoute Firewall.

Основы работы Kerio WinRoute Firewall

Kerio WinRoute Firewall представляет собой комплексную систему по организации корпоративного доступа к Интернету. По сути, он является полнофункциональным прокси-сервером, тесно интегрированным с целым рядом инструментов для защиты информационной системы предприятия от внешних угроз.

Kerio WinRoute Firewall инсталлируется на интернет-шлюз или любой другой компьютер, играющий его роль. Сам процесс установки прост и понятен, а с настройкой дела обстоят сложнее. Для ее выполнения необходимо обладать определенными знаниями. Впрочем, в этом нет абсолютно ничего удивительного. Все-таки рассматриваемый продукт является корпоративной системой, рассчитанной на обслуживание ИТ-специалистами. Если рассмотреть процесс настройки с их точки зрения, то его можно назвать удобным. Во-первых, он может осуществляться не только локально, но и удаленно с помощью специального приложения — «Консоли администрирования». Это позволяет сотрудникам ИТ-отдела управлять всеми параметрами и оперативно реагировать на любые инциденты, не вставая со своего рабочего места. Во-вторых, практически вся работа с консолью осуществляется в одном окне, а параметры сервера разбиты на группы, представленные в виде древовидного списка. Такой подход наиболее прост и удобен для пользователя. В-третьих, у Kerio WinRoute Firewall есть руководство администратора, в котором подробно расписаны все аспекты настройки и использования этого продукта.

Организовываем доступ в Интернет

Как мы уже говорили, Kerio WinRoute Firewall — полноценный прокси-сервер, позволяющий организовать многопользовательский доступ к одному или нескольким интернет-каналам. Для этого в нем реализованы такие функции, как DHCP-сервер, технология NAT и переадресация DNS-запросов. Благодаря им можно организовать доступ к Интернету любых сетевых приложений. Отдельно стоит отметить поддержку VoIP-трафика. Все-таки сегодня многие компании используют IP-телефонию, а поэтому этот момент достаточно важен . Настроить прокси-сервер можно вручную или воспользоваться специальным пошаговым мастером.

После настройки основных параметров прокси-сервера необходимо создать базу данных пользователей, которые смогут выходить в Интернет через него. Сделать это можно вручную. Однако гораздо быстрее и удобнее импортировать учетные записи из Active Directory или домена Windows NT. Кстати, в программе существует два варианта

аутентификации пользователей. Первый предполагает использование собственной базы данных, а второй — Active Directory. Таким образом, внесение и настройка сотрудников компании максимально облегчена.

Следующий момент, на который стоит обратить внимание — настройка системы ограничения полосы пропускания. Она используется для решения сразудвух задач. Первая — уменьшение нагрузки на интернет-канал за счет контроля и ограничения некритичного трафика, вторая — обеспечение бесперебойной работы важных или чувствительных к сбоям сетевых приложений. В рамках этой системы реализовано сразу несколько инструментов. Во-первых, это искусственное ограничение скорости при загрузке или отдаче большого (порог задается администратором) объема информации. Оно очень тонко настраивается. В частности, можно явно указать протоколы, адреса и службы на которые оно будет или, наоборот, не будет распространяться. В результате можно сделать так, чтобы, например, загружаемые пользователями «тяжелые» файлы не мешали работе IP-телефонии.

Во-вторых, в систему ограничения полосы пропускания входит лимитация дневного, недельного и месячного трафика как отдельных пользователей, так и целых их групп. Причем администратор сам выбирает, какие санкции применить к превысившим любой из порогов сотрудникам. Так, можно полностью заблокировать их доступ или же просто снизить до нужного значения доступную им полосу пропускания.

Помимо этого в рассматриваемом прокси-сервере реализован целый ряд других возможностей: кеширование информации, ведение подробного журнала, оповещение администратора о различных событиях и многое, многое другое.

Настраиваем защиту

Для защиты корпоративной сети от внешних угроз в Kerio WinRoute Firewall реализован целый ряд инструментов. Естественно, все они требуют внимания со стороны администратора. Первый из них — система фильтрации трафика. Она состоит сразу из трех подсистем. Начать нужно с политики HTTP. С ее помощью можно заблокировать доступ к нежелательным сайтам и объектам. Задавать их можно несколькими способами: ручным вводом адресов, указанием «стоп-слов» (слов, наличие которых на сайте приведет к блокировке последнего), а также при помощи Kerio Web Filter. О последнем варианте стоит сказать особо. Дело в том, что он позволяет блокировать сайты по категориям. Например, администратор может запретить доступ ко всем игровым порталам, социальным сетям, спортивным и автомобильным ресурсам и пр. Это позволяет не только существенно уменьшить риск заражения рабочих станций вредоносным ПО (как известно, сайты некоторых категорий часто используются для распространения вирусов и троянских коней), но и повысить производительность труда сотрудников компании. Второй инструмент — политика FTP. С ее помощью можно запретить загружать на FTP-сервера или скачивать с них файлы определенных расширений. Особо стоит отметить, что обе эти политики очень гибки. Администратор может установить свои правила для разных пользователей и групп пользователей, а также различных временных интервалов.

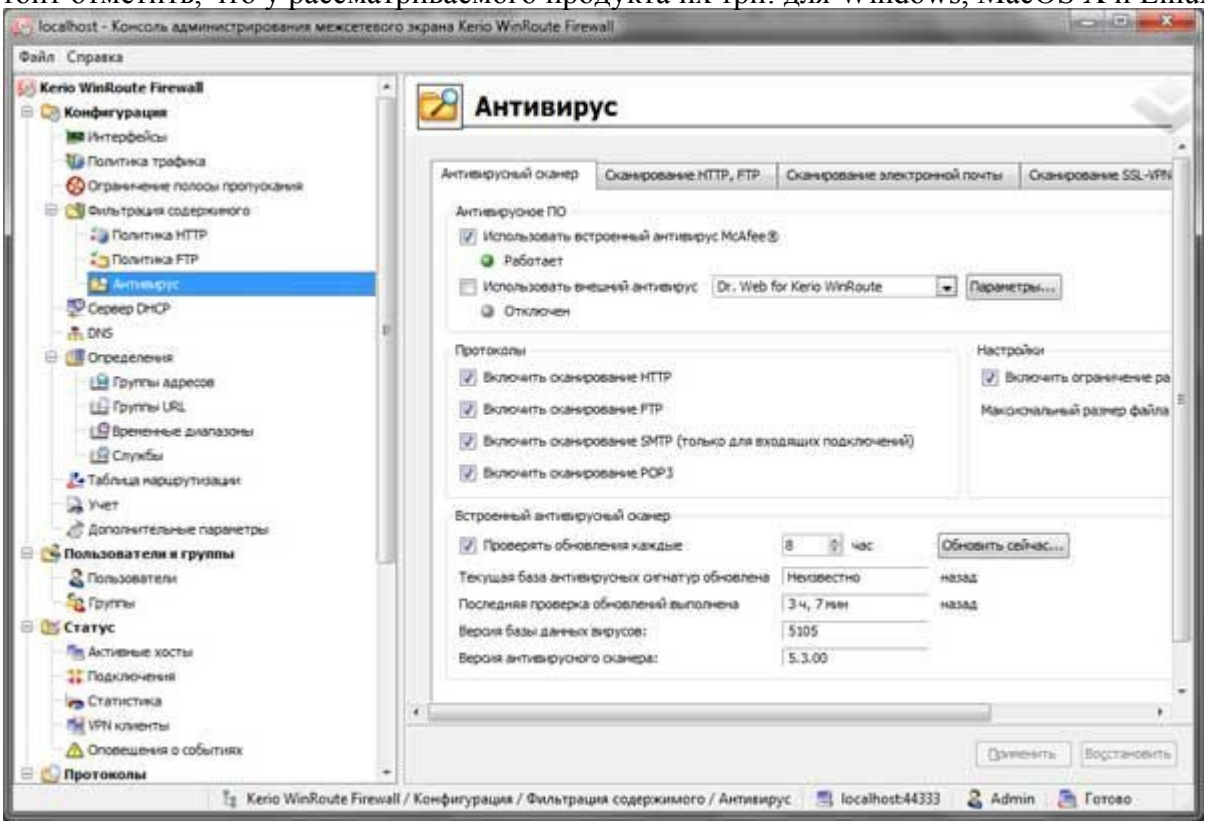
Третий инструмент в системе фильтрации трафика — защита от вредоносного ПО. Здесь нужно отметить один момент. У Kerio WinRoute Firewall существует два варианта поставки: со встроенным сканером McAfee и без него. Кроме того, в программе реализована возможность использования внешнего антивирусного ПО (Dr.Web, Nod32, Avast и пр.). Дополнительные антивирусные модули нужно приобретать отдельно. Таким образом, Kerio WinRoute Firewall, фактически, может работать в четырех режимах: без антивируса, только со встроенной или только с внешней защитой или с двойным сканированием (последовательно встроенным и внешним антивирусом).

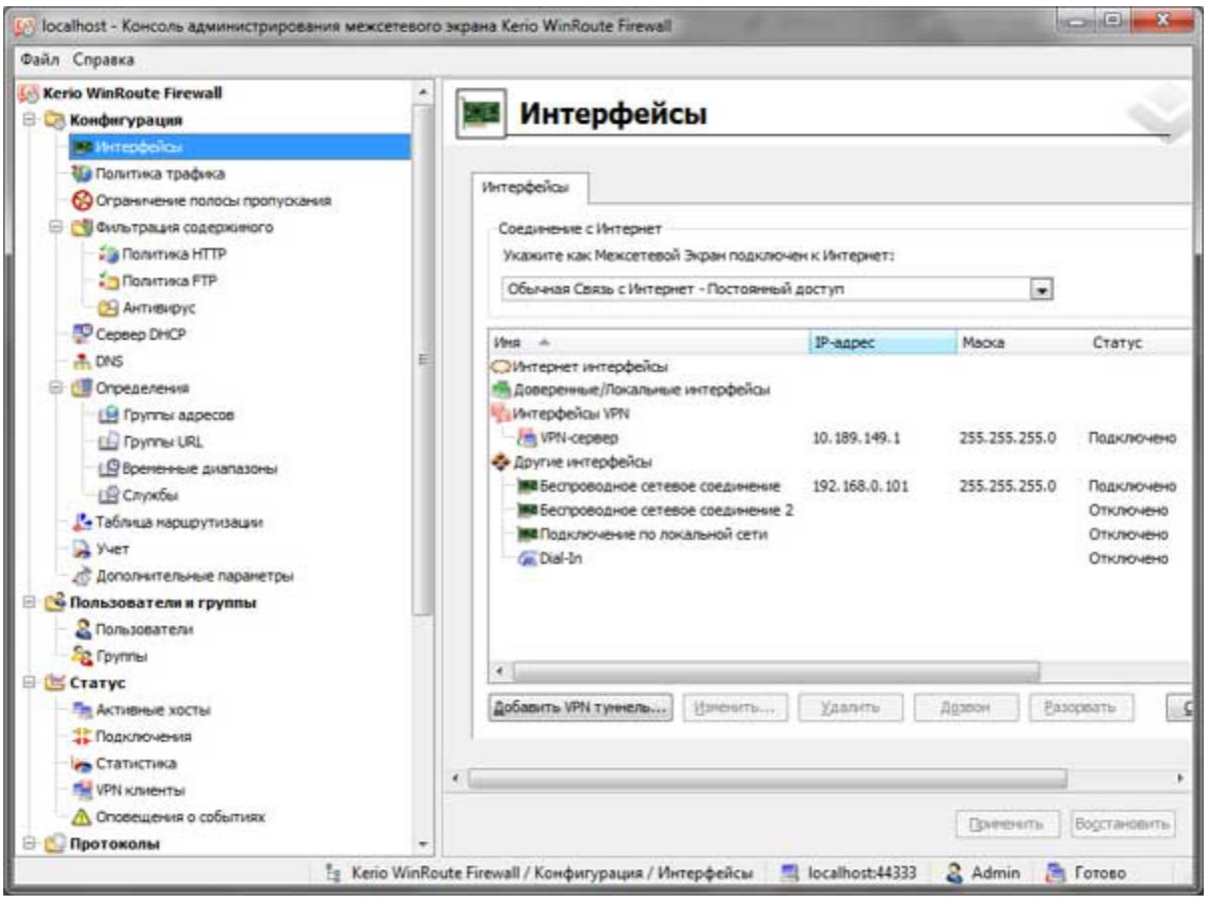
Следующий инструмент защиты — файрволл, работающий на уровне приложений. Он позволяет очень гибко настраивать политику обработки входящего и исходящего трафика. В правилах файрволла в качестве источника и приемника можно назначать

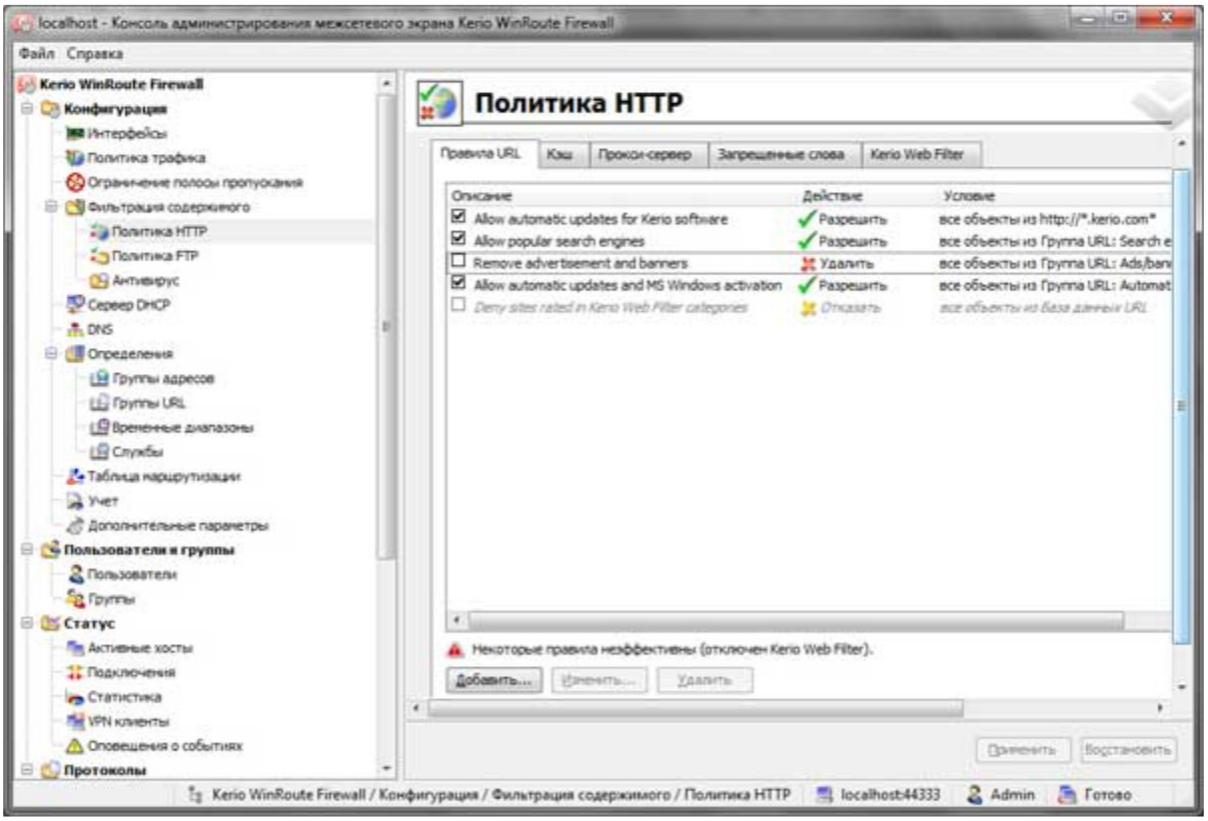
любые хосты, IP-адреса (в том числе их диапазоны и группы), сети, пользователей, входящих VPN-клиентов.

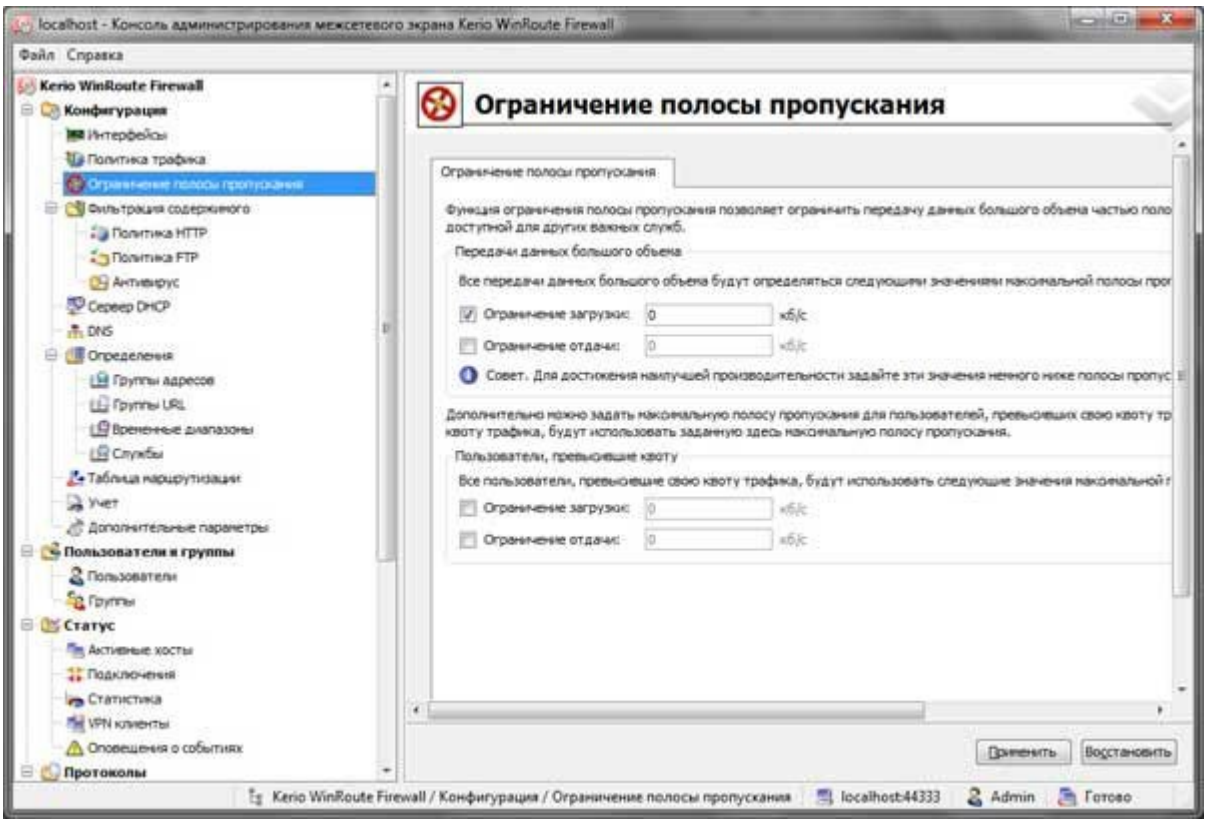
В дополнительных параметрах «Консоли администрирования» можно найти еще один важный для обеспечения информационной безопасности компании инструмент. Речь идет о фильтре P2P-трафика. Это весьма интересное решение, построенное на основе анализа трафика и могущее обнаруживать даже скрытое использование пиринговых сетей. Это немаловажно. Дело в том, что современные P2P-сети очень часто используются для распространения вредоносного ПО. Кроме того, потенциально они могут стать причиной утечки конфиденциальной информации. Именно поэтому рекомендуется активировать данные фильтр и настроить его параметры: выбрать тип реакции на обнаружение пирингового трафика (заблокировать только P2P или весь трафик указанного хоста). Если же запрещать пиринговые сети не планируется, то можно ограничить доступную им полосу пропускания, причем не только на загрузку, но и на выгрузку информации.

Наконец, последний инструмент, который особо хочется отметить — полноценный VPN-сервер, входящий в состав Kerio WinRoute Firewall. Его можно использовать как для подключения удаленных офисов компании, так и для работы отдельных пользователей. В первом случае необходимо установить в каждом из офисов Kerio WinRoute Firewall и организовать VPN-канал между ними. В результате все локальные сети будут интегрированы друг с другом. Во втором случае необходимо использовать VPN-клиент. Стоит отметить, что у рассматриваемого продукта их три: для Windows, MacOS X и Linux.




localhost - Консоль администрирования межсетевого экрана Kerio WinRoute Firewall
Файл Справка
Kerio WinRoute Firewall
Конфигурация
Интерфейсы
Политика трафика
Ограничение полосы пропускания
Фильтрация содержимого
Политика HTTP
Политика FTP
Антивирус
Сервер DHCP
DNS
Определения
Группы адресов
Группы URL
Временные диапазоны
Службы
Таблица маршрутизации
Учет
Дополнительные параметры
Пользователи и группы
Пользователи
Группы
Статус
Активные хосты
Подключения
Статистика
VPN клиенты
Оповещения о событиях
Протоколы
Интерфейсы
Соединение с Интернет
Укажите как Межсетевой Экран подключен к Интернет:
Обычная Связь с Интернет - Постоянный доступ
Имя
IP-адрес
Маска
Статус
Интернет интерфейсы
Доверенные/Локальные интерфейсы
Интерфейсы VPN
VPN-сервер
10.189.149.1
255.255.255.0
Подключено
Другие интерфейсы
Беспроводное сетевое соединение
192.168.0.101
255.255.255.0
Подключено
Беспроводное сетевое соединение 2
Отключено
Подключение по локальной сети
Отключено
Dial-In
Отключено
Добавить VPN туннель...
Изменить...
Удалить
Дозвон
Разорвать
Применить
Восстановить
Kerio WinRoute Firewall / Конфигурация / Интерфейсы
localhost:44333
Admin
Готово


localhost - Консоль администрирования межсетевого экрана Kerio WinRoute Firewall
Файл Справка
Kerio WinRoute Firewall
Конфигурация
Интерфейсы
Политика трафика
Ограничение полосы пропускания
Фильтрация содержимого
Политика HTTP
Политика FTP
Антивирус
Сервер DHCP
DNS
Определения
Группы адресов
Группы URL
Временные диапазоны
Службы
Таблица маршрутизации
Учет
Дополнительные параметры
Пользователи и группы
Пользователи
Группы
Статус
Активные хосты
Подключения
Статистика
VPN клиенты
Оповещения о событиях
Протоколы
Политика HTTP
Правила URL
Кэш
Прокси-сервер
Запрещенные слова
Kerio Web Filter
Описание
Действие
Условие
Allow automatic updates for Kerio software
Разрешать
все объекты из http://*.kerio.com*
Allow popular search engines
Разрешать
все объекты из Группа URL: Search e
Remove advertisement and banners
Удалить
все объекты из Группа URL: Ads/ban
Allow automatic updates and MS Windows activation
Разрешать
все объекты из Группа URL: Automat
Deny sites rated in Kerio Web Filter categories
Отказать
все объекты из база данных URL
Некоторые правила неэффективны (отключен Kerio Web Filter).
Добавить...
Изменить...
Удалить
Применить
Восстановить
Kerio WinRoute Firewall / Конфигурация / Фильтрация содержимого / Политика HTTP
localhost:44333
Admin
Готово



Практическая часть

1. Установить программу X Spider
2. Отсканировать машину без защиты файрволом
3. Установить Kerio Personal Firewall
4. Отсканировать машину с установленным файрволом
5. Проанализировать полученные результаты и произвести настройку файрвола для устранения найденных уязвимостей
6. Объяснить природу обнаруженных уязвимостей

Контроль выполнения задания производится по окончании занятия и на консультациях в форме защиты выполненной работы, предоставленной в электронном и в бумажном виде в форме «Отчет по лабораторной работе».

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы
1-2	1-2	1-2	1-4

Оценочные средства: отчет к лабораторной работе (См.: Фонд оценочных средств)

Лабораторная работа №2 «Принципы построения VPN сети (VipNet)»

Форма проведения: лабораторная работа

Цель работы:

Ознакомиться с принципами построения VPN сети (VipNet).

Теоретические сведения

Многие VPN-системы предназначены главным образом для безопасного соединения локальных сетей через Интернет и организации защищенного удаленного доступа к ресурсам. В случае, если наряду с данными задачами есть задача организации защиты трафика напрямую между узлами независимо от их месторасположения, в том числе внутри локальной сети, по схеме Peer-to-Peer, то использование таких систем сильно затрудняется. Технология ViPNet позволяет легко решить задачи VPN-связности узлов в любых топологиях.

Одним из выгодных отличий технологии ViPNet от классических VPN-систем является отсутствие каких-либо процедур синхронизации и выработки ключей в процессе сеансов обмена защищенной информацией между узлами ViPNet. Это свойство значительно повышает устойчивость системы и обеспечивает высокую надежность работы различных сетевых служб.

1.1 Компоненты виртуальной сети ViPNet

Виртуальная сеть строится с использованием компонентов ViPNet для различных операционных систем, программно-аппаратных комплексов ViPNet, а также готовых виртуальных машин для различных виртуальных сред. В виртуальную сеть могут включаться также мобильные устройства на платформах iOS, Android и других ОС, на которых установлены приложения ViPNet Client, разработанные для данных платформ.

Компьютеры и мобильные устройства с ПО ViPNet Client в дальнейшем именуются Клиентами. Клиенты обеспечивают сетевую защиту и включение в VPN-сеть отдельных компьютеров и устройств.

Компьютеры с ПО ViPNet Coordinator для Windows и Linux, программно-аппаратные комплексы ViPNet для больших и мелких сетей, индустриальные шлюзы безопасности различной мощности, координаторы ViPNet на виртуальных машинах в дальнейшем именуются Координаторами. Координаторы различного класса защищенности обеспечивают шифрование трафика туннелируемых ими сетевых ресурсов (как VPN-шлюзы), ретранслируют VPN-трафик между другими VPN-узлами, выполняют служебные функции по поддержанию связности защищенной сети и оптимизации маршрутов прохождения VPN-трафика между узлами.

Клиенты и Координаторы называются узлами виртуальной сети ViPNet или просто узлами ViPNet. Возможность обмена трафиком через защищенные каналы между узлами ViPNet (связи между узлами) централизованно задает администратор.

1.2 Функции координатора

Координаторы, как правило, устанавливаются на границе сетей и выполняют следующие функции:

- VPN-шлюз — стандартная для классических VPN функция, реализующая создание защищенных каналов (туннелей) site-to-site и client-to-site между локальными и удаленными узлами. Координатор может создавать такой канал через каскад других координаторов, выполняющих функцию маршрутизации VPN-пакетов.
- Межсетевой экран — функция фильтрации открытых, защищенных и туннелируемых транзитных и локальных сетевых соединений, а также функция трансляции адресов для открытых и туннелируемых соединений.
- Сервер IP-адресов — функция автоматического обмена актуальной информацией о топологии сети между узлами ViPNet как внутри данной виртуальной сети, так и при взаимодействии с узлами других виртуальных сетей ViPNet. Обмен информацией осуществляется с помощью специального защищенного протокола динамической маршрутизации VPN-трафика (см. «Протокол динамической маршрутизации»). Результатом работы данного протокола является возможность маршрутизации VPN-трафика между узлами сети

ViPNet по маршруту, оптимальному для используемого способа и места подключения узла к сети.

- Маршрутизатор VPN-пакетов — функция, обеспечивающая маршрутизацию транзитного VPN-трафика, проходящего через координатор на другие узлы ViPNet. Маршрутизация осуществляется на основании идентификаторов защищенных узлов, передаваемых в открытой части VPN-пакетов и защищенных от подделки имитовставкой, и на основании данных, полученных в результате работы протокола динамической маршрутизации VPN-трафика. Любой VPN-трафик, прошедший на координаторе маршрутизацию, отправляется на следующий или конечный узел ViPNet на IP-адрес и порт, по которому этот узел доступен. IP-адрес источника пакета заменяется на адрес интерфейса координатора, с которого ушел пакет. При работе в роли маршрутизатора VPN-пакетов координатор не имеет доступа к самим зашифрованным данным других узлов, а только выполняет их пересылку.
- Если клиент или координатор подключается к Интернету через устройство с динамическим NAT, то они недоступны напрямую для входящих инициативных соединений других узлов. В этом случае для организации доступа к ресурсам корпоративной сети за этим координатором или для соединения с таким клиентом с удаленных узлов один из координаторов во внешней сети определяется для них как сервер соединений, с которым они поддерживают постоянную связь. За счет функционала маршрутизатора VPN-пакетов сервер соединений служит промежуточным звеном для установления связи с таким узлом из внешней сети (с возможностью последующего перехода на прямое общение, подробнее см. «Соединение двух узлов, которые подключаются к Интернету через устройства с динамическим NAT»).
- Сервер соединений автоматически задается в настройках клиентов при их развертывании, и впоследствии его можно менять. Для координатора при необходимости сервер соединений можно задать в его настройках.
- Транспортный сервер — функция, которая обеспечивает доставку обновлений ключей, справочной информации, политик, обновлений ПО ViPNet из программ управления сетью ViPNet на защищенные узлы, а также маршрутизацию почтовых конвертов прикладного ПО ViPNet (например, программ ViPNet Деловая почта, Файловый обмен).

По умолчанию сервер IP-адресов является сервером соединений для клиента. При необходимости сервером соединений может быть назначен другой координатор.

2. Общие принципы взаимодействия узлов ViPNet в виртуальной сети

Узлы сети ViPNet могут располагаться в сетях любого типа, поддерживающих IP-протокол. Способ подключения узла к сети может быть любой: сеть Ethernet, PPPoE через XDSL-подключение, PPP через подключение Dial-up или ISDN, любая сеть сотовой связи, устройства Wi-Fi, сети MPLS или VLAN и другие.

2.1 Протокол динамической маршрутизации

Два узла в сети ViPNet могут взаимодействовать друг с другом, если администратор задал между ними связи в управляющем приложении (ViPNet Administrator). Для доступа к удаленным туннелируемым узлам нужно задать связь с туннелирующим их координатором. Задание связи между двумя узлами означает появление у двух узлов необходимой ключевой информации для организации защищенного VPN-соединения между ними.

У каждого клиента есть «свой» координатор — его сервер IP-адресов, сервер соединений и транспортный сервер (см. «Функции координатора». При необходимости можно настроить выполнение этих функций разными координаторами).

Постоянную возможность доступа узлов ViPNet друг к другу обеспечивает протокол динамической маршрутизации VPN-трафика, работающий на прикладном

уровне ОС. Обмен служебными данными в рамках этого протокола происходит через те же VPN-соединения и, таким образом, защищен.

Работа протокола динамической маршрутизации заключается в автоматической передаче между узлами сети ViPNet актуальной информации о возможных способах доступа друг к другу, а также списков своих реальных IP-адресов. Протокол распространяет эту информацию не только в рамках своей сети ViPNet, но и также между узлами разных сетей ViPNet (если администраторы двух сетей договорились и обменялись между собой соответствующей информацией о связях между узлами двух сетей для защищенного взаимодействия в соответствии со своими задачами).

Ключевую роль в работе протокола играют координаторы, которые и обеспечивают все узлы сети необходимой информацией для организации связи. Выполняя функцию сервера IP-адресов, координаторы собирают информацию об актуальных способах доступа к «своим» клиентам. Далее серверы IP-адресов передают эту информацию на связанные с их клиентами узлы, напрямую или через некоторую цепочку других координаторов.

Для обеспечения защищенной передачи трафика в соответствии с задачами информационного обмена (далее целевого трафика) нужно задать связи между узлами, обеспечивающими защиту этого трафика (клиентами и туннелирующими координаторами), а также задать связи клиентов со «своими» координаторами, которые в большинстве случаев создаются автоматически.

Для обеспечения защищенной передачи трафика протокола динамической маршрутизации (далее служебного трафика) требуется также задать связи между координаторами, по цепочке которых должна передаваться информация о доступе к узлам. В небольших сетях для простоты можно связать координаторы по принципу «все со всеми». Однако в больших сетях с целью сокращения служебного трафика число связей между координаторами следует минимизировать и задавать связи исходя из следующих возможностей маршрутизации служебного трафика:

- В рамках одной сети ViPNet информация передается по цепочке, в которой присутствует не более двух координаторов. То есть, если клиенты связаны между собой, то должны быть связаны между собой и координаторы, которые выполняют для этих клиентов функции сервера IP-адресов.
- При взаимодействии двух разных сетей ViPNet обмен служебным трафиком может происходить по цепочке до двух координаторов в каждой из сетей. Благодаря этому в каждой сети достаточно выделить один координатор (шлюзовой), через который будет происходить обмен с другой сетью, и связать его с таким же координатором в другой сети. А уже с этими координаторами связываются координаторы каждой из сетей, которые должны передать служебную информацию в другую сеть. При такой топологии шлюзовые координаторы становятся «единой точкой входа» в другую сеть, что упрощает и управление, и контроль межсетевого обмена. Естественно, если координаторы двух сетей связать напрямую, а не через выделенные шлюзовые координаторы, то информация будет передаваться более коротким путем.

В результате работы протокола динамической маршрутизации все узлы ViPNet владеют информацией о параметрах доступах к другим узлам, с которыми связаны. При этом во всех случаях целевой трафик между узлами независимо от маршрута служебного трафика пойдет кратчайшим путем, минуя координаторы, если это позволяет существующая сетевая инфраструктура (см., например: «Соединение двух узлов, которые подключаются к Интернету через устройства с динамическим NAT»).

2.2 Инкапсуляция

ПО ViPNet перехватывает весь сетевой трафик клиента или координатора. Трафик, предназначенный для передачи через защищенный канал на другой узел ViPNet,

инкапсулируется в защищенные ViPNet IP-пакеты. Инкапсулируются исходные IP-пакеты любых протоколов (туннелирование на сетевом уровне).

При появлении любого IP-пакета в адрес других узлов ViPNet, с которыми есть связь, пакет без каких-либо протоколов предварительного установления соединений с узлом-получателем шифруется, инкапсулируется в ViPNet-пакет и передается через VPN-сеть на узел-получатель.

Определенные модификации координаторов также поддерживают построение туннелей на канальном уровне (L2 OSI), что позволяет объединить в единую локальную сеть удаленные сегменты сетей. В этом случае в защищенные ViPNet IP-пакеты (UDP-протокол) инкапсулируются Ethernet-кадры любых сетевых протоколов, а не только IP.

Для инкапсуляции в ViPNet-пакеты используются два типа IP-протокола:

- IP/UDP с портом источника 55777 по умолчанию или любым другим портом, который автоматически регистрируется на других узлах.
- IP/241 — используется при взаимодействии узлов в одной локальной сети.

Для взаимодействия узлов в одном широковещательном домене автоматически используется протокол IP/241, у которого меньше накладные расходы благодаря отсутствию дополнительных UDP-заголовков.

Для инкапсуляции трафика между узлами в одном широковещательном домене используется протокол IP/241

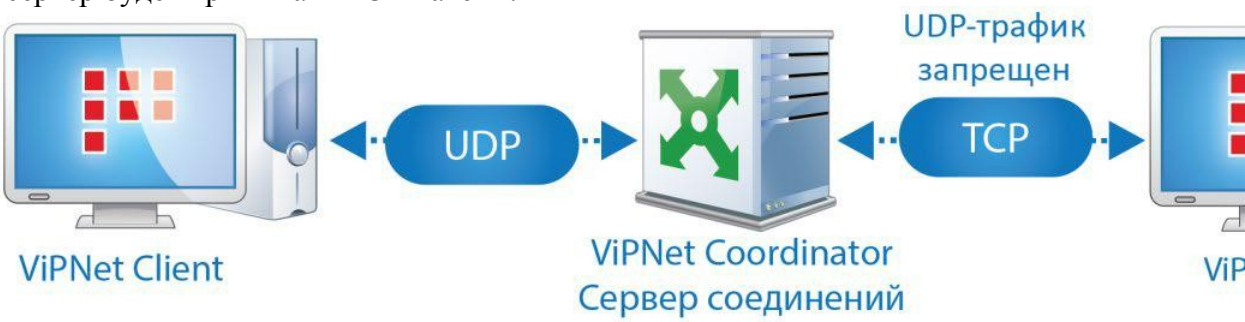
В других случаях автоматически используется протокол UDP, для которого легко организовать прохождение IP-пакетов через любые типы межсетевых экранов и устройства с NAT. При формировании защищенных UDP-пакетов узлы по умолчанию задают порт источника 55777 (порт инкапсуляции), но в их настройках можно задать произвольный порт, который благодаря протоколу динамической маршрутизации станет известен и другим узлам для организации доступа по этому порту. При прохождении через устройства NAT в сети порт источника в пакетах может поменяться. Информация об этом также станет известной другим узлам для организации прохождения встречного трафика.

Для инкапсуляции трафика между узлами, разделенными NAT-устройством, используется UDP-протокол

Бывают случаи, когда передача UDP-пакетов запрещена Интернет-провайдером, и взаимодействие защищенных узлов по UDP-протоколу невозможно. Например, UDP-трафик бывает запрещен при использовании точек доступа в гостиницах и других общественных местах.

Узел автоматически определяет такой запрет и устанавливает с сервером соединений TCP-соединение (по умолчанию по порту 80), через которое передает

сформированные UDP-пакеты. ViPNet-трафик для других узлов передается через это соединение на сервер соединений, откуда уже в обычном виде передается дальше. При настройке TCP-туннеля на сервере соединений может быть указан любой порт, на котором сервер будет принимать TCP-пакеты.



Если использование UDP-трафика невозможно, узел устанавливает соединение по протоколу TCP со своим сервером соединений и через него обменивается UDP-трафиком с другими узлами сети ViPNet

2.3 Первоначальные настройки защищенной сети

Всю информацию, необходимую для взаимодействия приложений, узлы получают автоматически за счет работы протокола динамической маршрутизации VPN-трафика. Первоначальные настройки, которые нужно сделать при развертывании сети, минимальны:

- В Центре управления сетью сформируйте структуру сети – клиенты, координаторы и их связи.
- Задайте IP-адреса или DNS-имена для доступа к координаторам сети.
- Клиенты ViPNet после инсталляции ПО в общем случае не требуют каких-либо настроек.
- Для каждого координатора при необходимости задайте один из нескольких режимов подключения к внешней сети. Режим по умолчанию («Со статической трансляцией адресов») в большинстве случаев обеспечивает его работу без дополнительных настроек. Подробнее о задании режимов подключения на координаторе см. раздел «Варианты подключения координаторов к внешней сети».
- На внешнем сетевом экране организации при необходимости настройте пропуск соответствующего протокола ViPNet (порты и адреса UDP-и/или TCP-протокола).
- Для взаимодействия с требуемыми узлами других сетей ViPNet обменяйтесь некоторой первичной служебной информацией с администратором другой сети ViPNet. В дальнейшем такой обмен будет происходить автоматически.

3. Механизмы соединений в сети ViPNet

3.1 Определение взаиморасположения узлов

Узлы по-разному устанавливают соединения, в зависимости от того, как они расположены по отношению друг к другу:

- Находятся в одном широковещательном домене.
- Находятся в одной маршрутизируемой сети, но в разных широковещательных доменах, то есть — разделены маршрутизирующими устройствами (в том числе со статической трансляцией адресов) и недоступны друг для друга по широковещательной рассылке.
- Разделены NAT-устройствами с динамической трансляцией адресов.

При подключении к сети или изменении собственного IP-адреса узел выполняет специальную широковещательную рассылку и по ответам определяет, какие другие узлы ViPNet находятся с ним в одном широковещательном домене. Такие узлы регистрируют IP-адреса друг друга. Пакеты, отправляемые по этим адресам, шифруются и инкапсулируются в протокол IP/241.

Для получения информации об узлах, недоступных в своем широковещательной домене, клиенты используют сервер IP-адресов, а для надежного первоначального соединения с ними используется сервер соединений, который владеет полным объемом информации о доступе к другим узлам.

3.2. Соединение двух узлов, которые подключаются к Интернету через устройства с динамическим NAT

Рассмотрим организацию соединений между двумя узлами, которые подключаются к сети Интернет через провайдера, предоставляющего доступ в Интернет в режиме динамического NAT. Например, Клиент 1 находится в гостинице в Лондоне, а Клиент 2 — в гостинице в Санкт-Петербурге:

1. При включении компьютера ПО ViPNet каждого из Клиентов определяет канал доступа к своему серверу соединений по UDP-протоколу (сервер соединений может быть и общий).

Если Клиенту 1 не удается соединиться со своим сервером соединений по UDP-протоколу, то Клиент устанавливает соединение по протоколу TCP (по умолчанию — порт 80, но можно установить и любой другой порт).

2. После подключения к серверу соединений клиент поддерживает соединение с ним путем периодической отправки на него тестовых IP-пакетов. Благодаря этому Клиент 1 предоставляет возможность другим узлам, в том числе и Клиенту 2, установить с ним инициативное соединение через свой сервер соединений. Интервал отправки IP-пакетов на сервер соединений по умолчанию равен 25 секундам. Этого, как правило, достаточно для работы через большинство устройств NAT. При необходимости интервал (тайм-аут) можно изменить.

3. Если от некоторого приложения на Клиенте 1 появляется целевой трафик в направлении Клиента 2 (например, VoIP), то Клиент 1 начинает передавать пакеты через свой сервер соединений. Сервер соединений, в свою очередь, пересылает эти пакеты на сервер соединений Клиента 2, а тот уже — самому Клиенту 2. Обратный трафик идет аналогичным маршрутом.

Если Клиент 1 соединяется со своим сервером соединений через TCP-соединение, то сервер соединений извлекает из TCP-соединения UDP-трафик (который по-прежнему зашифрован и недоступен для расшифрования на сервере соединений). Сервер передает UDP-трафик Клиенту 2 через его сервер соединений. Если Клиент 2 поддерживает связь со своим сервером соединений через TCP, то трафик, дойдя до сервера соединений Клиента 2, пойдет к Клиенту 2 через это TCP-соединение.

Таким образом, два клиента устанавливают связь друг с другом через два сервера соединений. Если клиент подключается к серверу соединений по UDP, то при благоприятной конфигурации сетевого окружения серверы соединений могут быть исключены из взаимодействия, то есть клиенты переходят к сообщению напрямую. Рассмотрим этот механизм:

1. Параллельно с началом передачи и приема целевого трафика по протоколу UDP через серверы соединений происходит следующее:

- Оба клиента через серверы соединений передают друг другу тестовый пакет с информацией о параметрах прямого доступа к себе из внешней сети (адрес и порт), полученной от своего сервера соединений.
- Оба клиента получают эти пакеты друг от друга и узнают о параметрах возможного прямого доступа друг к другу. Кроме того, каждый клиент также владеет информацией о доступе к серверу соединений другого клиента (эту информацию они получают заранее от своих серверов IP-адресов). Используя эти данные, оба клиента передают тестовые IP-пакеты напрямую на адреса и порты доступа друг к другу и к серверам соединений другой стороны.

1. Если тестовый IP-пакет хотя бы одной из сторон сумел пройти напрямую через NAT-устройство другой стороны, то между узлами устанавливается прямое соединение.

Доступность этого прямого соединения для обеих сторон сохраняется в течение 75 секунд после окончания передачи целевого трафика. После этого маршруты сбрасываются, а при необходимости установить соединение узлы опять начинают передачу трафика через свои серверы соединений.

Не все типы NAT позволяют установить прямое соединение (см. ниже). Прямое соединение возможно, если хотя бы у одной из сторон используется устройство NAT, позволяющее это сделать.

2. Если тестовые прямые IP-пакеты не дошли ни до одной из сторон, но дошли до сервера соединений другой стороны, то целевой трафик между двумя клиентами будет идти через один из серверов соединений. Доступность этого соединения также сохраняется для соединяющихся узлов в течение 75 секунд после окончания передачи целевого трафика. Аналогичная ситуация возникает, если один из клиентов подключается к своему серверу соединений через TCP. Этот сервер соединений не может быть исключен из передачи трафика, но может быть исключен другой сервер соединений, к которому его узел подключен по UDP.

3. Если тестовые пакеты никуда не дошли, то трафик между двумя узлами так и продолжит идти по длинному маршруту через два сервера соединений.

Начало взаимодействия клиентов за NAT-устройствами через серверы соединений и переход к взаимодействию напрямую

Существует четыре типа динамического NAT: Cone NAT, Address-Restricted cone NAT (или Restricted cone NAT), Port-Restricted cone NAT, Symmetric NAT. Установка прямого соединения не поддерживается только в случае, если оба NAT-устройства настроены для выполнения Symmetric NAT. В этом случае трафик будет идти через один из серверов соединений. Если хотя бы у одной стороны выполняется другой тип NAT, то прямое соединение будет установлено.

Таким образом, с удаленным узлом устанавливается либо прямое соединение, либо соединение через один из серверов соединений. Если существует возможность, узлы устанавливают взаимодействие друг с другом по кратчайшим маршрутам без участия их серверов соединений, за счет чего повышается скорость обмена шифрованным IP-трафиком и снижается нагрузка на координаторы. Если клиентам не удается установить более короткое соединение, то клиенты по-прежнему продолжают обмен между собой через свои серверы соединений.

3.3 Соединение узлов в одной маршрутизируемой сети

Если два клиента находятся в одной маршрутизируемой сети или разделены устройствами со статическим NAT, но недоступны друг для друга по широковещательной рассылке, первые пакеты они также отправляют через сервер соединений. После этого по описанному выше механизму (см. «Соединение двух узлов, которые подключаются к

Интернету через устройства с динамическим NAT») такие узлы гарантированно переходят к общению напрямую, без участия сервера соединений. Последующие соединения два узла устанавливают в соответствии с сохраненной информацией о маршрутизации без участия сервера соединений напрямую.

Узлы сохраняют информацию о маршрутизации пакетов друг для друга, которая не будет сброшена даже при отсутствии целевого трафика. Информация сбрасывается, только если узел будет отключен и затем заново подключен к сети.

3.4 Выбор сервера соединений для клиента, который перемещается в другую сеть ViPNet

Пользователь клиента или администратор сети может выбирать для клиента в качестве сервера соединений любой координатор, в том числе — координатор в другой сети ViPNet, с которой установлено межсетевое взаимодействие. Это бывает нужно, например, если клиент перемещается в локальную сеть, из которой доступ в Интернет возможен только через расположенный в этой локальной сети «чужой» координатор (координатор другой сети ViPNet). Условием возможности подключения через сервер соединений в другой сети является:

- наличие межсетевого взаимодействия между сетью клиента и сетью сервера соединений;
- связь «чужого» сервера соединений с координатором в «своей» сети, выполняющим для клиента роль сервера IP-адресов.

Задача сервера соединений — обеспечить соединения клиента с узлами, с которыми клиент связан. Для этого сервер соединений должен владеть информацией о возможных путях доступа к этим узлам, чтобы обеспечить маршрутизацию целевого трафика клиента. Однако в чужую сеть (сеть сервера соединений) информация о параметрах доступа к узлам других сетей может попасть, только если эти узлы связаны с какими-либо узлами этой чужой сети. Чаще всего это не так, и хотя бы некоторые (а возможно — и все) узлы, с которым связан клиент, и к которым клиенту может потребоваться доступ, не имеют связи с этой сетью. Зато информацией о доступе к этим узлам владеет сервер IP-адресов клиента в его сети. Сервер IP-адресов передает ее на клиент. Получив эту информацию, клиент пересылает ее серверу соединений в чужой сети. В результате сервер соединений в чужой сети может выполнить маршрутизацию целевого трафика клиента для всех узлов, с которыми он связан. Клиент получает доступ ко всем ресурсам своей и других защищенных сетей, с которыми связан.

Если исходный сервер соединений клиента доступен из локальной сети, в которую переместился клиент, то необходимости менять сервер соединений не возникает.

4. Варианты подключения координаторов к внешней сети

Для координатора можно задать один из нескольких режимов подключения в внешней сети. Выбор режима зависит от того, отделен ли координатор от внешней сети внешним по отношению к координатору межсетевым экраном. Можно установить следующие режимы:

- Режим подключения «Без использования межсетевого экрана».
- Режим подключения «За координатором», при котором внешним межсетевым экраном является другой координатор.
- Режим подключения через межсетевой экран «Со статической трансляцией адресов».
- Режим подключения через межсетевой экран «С динамической трансляцией адресов».

По умолчанию координаторы устанавливаются в режим работы через межсетевой экран «Со статической трансляцией адресов». Режим можно изменить в управляющем приложении ViPNet Administrator или непосредственно на координаторе. Этот режим достаточно универсален и может использоваться в большинстве случаев.

4.1 Подключение координатора в режиме «Без использования межсетевого экрана»

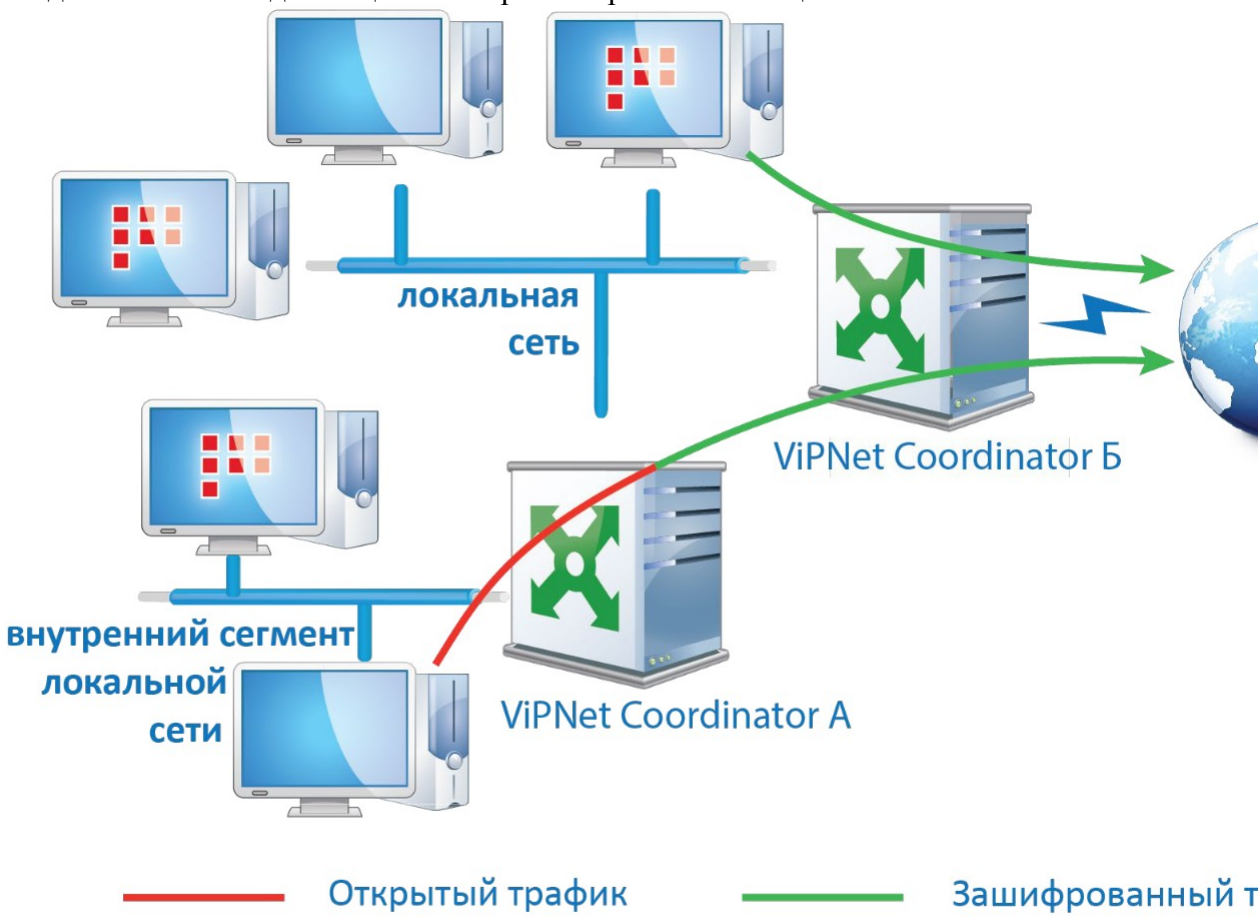
Если координатор имеет постоянный IP-адрес в Интернете, то к нему можно построить маршрут из любой сети, имеющей доступ в Интернет. На таком координаторе можно установить режим «Без использования межсетевого экрана».

В этом случае может использоваться и режим по умолчанию «Со статической трансляцией адресов». В последующих версиях ViPNet режим «Без использования межсетевого экрана» предполагается исключить из использования.

4.2 Подключение координатора через другой координатор: режим «За координатором»

Если координатор А расположен на границе между внутренним и внешним сегментами локальной сети, а внешняя сеть защищена координатором Б, то координатор А обычно устанавливают в режим «За Координатором», выбрав в качестве внешнего координатора координатор Б. Координатор Б в этом случае выполняет для координатора А роль сервера соединений.

Такая установка координаторов в цепочку друг за другом (каскадирование) позволяет защитить трафик внутренних сегментов локальной сети как во внешнем контуре локальной сети, так и при выходе трафика за ее пределы. Количество координаторов в цепочке не ограничивается. За один координатор можно установить несколько координаторов и тем самым обеспечить надежную изоляцию друг от друга и от общей локальной сети нескольких ее сегментов. В любой точке этой локальной сети могут находиться клиенты для защиты конкретных рабочих станций.



Каскадное включение координаторов

При установке координаторов внутри локальной сети за координатор, стоящий на е границе (каскадное включение координаторов) трафик из внутреннего сегмента локальной сети на удаленные узлы ViPNet передается следующим образом:

- Координаторы ViPNet, защищающие внутренние сегменты локальной сети, автоматически отправляют зашифрованный ими трафик, предназначенный

удаленным защищенным ресурсам, на координатор на границе внешнего сегмента сети. Этот координатор отправляет защищенный трафик дальше в соответствии с имеющейся у него информацией об удаленных узлах.

- Удаленные узлы ViPNet отправляют трафик, предназначенный для внутреннего сегмента локальной сети, через внешний координатор, который перенаправляет его дальше, координаторам внутри локальной сети.

Каскадное включение координаторов позволяет защитить трафик внутреннего сегмента локальной сети при его прохождении как во внешнем сегменте локальной сети, так и во внешней публичной сети. Каскадирование также позволяет пропустить VPN-трафик по нужному маршруту в глобальной сети, что часто используется для его контроля в различных схемах администрирования.

Построение схемы с каскадированием координаторов не ограничено настройкой координаторов в режиме «За координатором». Такую же схему можно создать путем использования режима координатора с динамическим NAT с настройкой «Весь трафик передавать через сервер соединений». В последующих версиях для построения каскадных схем планируется использовать только этот режим координатора.

4.3 Подключение координатора через межсетевой экран «Со статической трансляцией адресов»

Если на границе локальной сети уже установлен межсетевой экран стороннего производителя с возможностью настройки статических правил трансляции адресов, то за ним можно расположить координатор с частными адресами сетевых интерфейсов и установить на нем режим межсетевого экрана «Со статической трансляцией адресов». Каждый из сетевых интерфейсов координатора может быть подключен к той или иной сети через отдельный межсетевой экран со статическими правилами трансляции. Через этот координатор будет обеспечено взаимодействие других узлов ViPNet и открытых узлов в локальной сети с узлами за ее пределами.

На межсетевом экране должны быть настроены статические правила трансляции адресов:

- Перенаправление пакетов из внешней сети на адрес координатора в соответствии с заданным на координаторе портом инкапсуляции трафика.
- Пропуск во внешнюю сеть UDP-пакетов, в которых в качестве источника указаны адрес и порт инкапсуляции координатора.

Работа координатора в режиме «Со статической трансляцией адресов»

Координатор в данном режиме успешно работает и при отсутствии реального внешнего межсетевого экрана. Поэтому такой режим устанавливается на координаторах по умолчанию.

4.1 Режим межсетевого экрана «С динамической трансляцией адресов»

Если координатор устанавливается на границе локальной сети, которая подключается к внешним сетям через межсетевые экраны с динамической трансляцией адресов, то нужно задать режим работы за межсетевым экраном «С динамической трансляцией адресов».

Поскольку координатор недоступен из внешней сети для инициативных соединений, то для него следует назначить в качестве сервера соединений один из координаторов, доступный из внешней сети (работающий в режиме «Со статической трансляцией адресов» или «Без использования межсетевого экрана»). Сервер соединений обеспечит возможность инициативного соединения с ресурсами локальной сети за таким координатором со стороны любых других узлов (с учетом связей в защищенной сети).

За счет того, что координатор в данном режиме доступен из внешней сети через его сервер соединений, клиенты и туннелируемые ресурсы в локальной сети за ним доступны для других узлов в полном объеме — так же, как за координатором в любом другом режиме. Работа координатора через сервер соединений в этом режиме аналогична описанной выше работе клиента за NAT-устройством и позволяет переходить к сообщению «напрямую», без участия сервера соединений (подробно о работе клиентов через сервер соединений см. «Соединение двух узлов, которые подключаются к Интернету через устройства с динамическим NAT»).

Работа координатора в режиме «С динамической трансляцией адресов» аналогична работе клиента за NAT-устройством: координатор гарантированно доступен из внешней сетичерез сервер соединений. Для простоты на рисунке не отображен сервер соединений удаленного клиента, который также участвует в первоначальном установлении соединения.

Если в настройках координатора включить опцию «Весь трафик передавать через сервер соединений», то можно строить каскадные схемы, аналогичные режиму «За координатором».

5. Туннелирование IP-трафика открытых ресурсов

Для включения в виртуальную сеть узлов локальной сети, трафик которых не требуется защищать в локальной сети, координатор выполняет функцию туннелирующего сервера (VPN-шлюза):

- Выступает шлюзом для передачи IP-трафика в сеть ViPNet, осуществляя инкапсуляцию и шифрование трафика открытых туннелируемых узлов.
- Обеспечивает взаимодействие туннелируемых узлов с удаленными узлами для любых IP-протоколов. При этом не имеет значения, согласованы ли

локальные адреса взаимодействующих узлов. Благодаря технологии виртуальных адресов в сети ViPNet могут взаимодействовать узлы, имеющие одинаковые IP-адреса (см. «Виртуальные адреса в сети ViPNet»), так что согласования адресации не требуется.

- Скрывает адресную структуру защищаемой локальной сети за счет того, что принимает и передает инкапсулированный трафик от имени своего IP-адреса.

Для соединения открытых туннелируемых ресурсов с любыми удаленными клиентами, координаторами или туннелируемыми узлами удаленной локальной сети доступны все вышеописанные схемы подключения координаторов к сети. Это позволяет использовать все преимущества виртуальной сети ViPNet в распределенных информационных сетях со сложной топологией.

Открытые узлы, которые данный координатор будет туннелировать, можно задавать в настройках координатора или в управляющем приложении ViPNet Administrator в виде отдельных адресов или диапазонов.

6. Виртуальные адреса в сети ViPNet

6.1 Принцип работы виртуальных адресов

Технология ViPNet обеспечивает взаимодействие между защищаемыми ресурсами, которые имеют частные IP-адреса, без согласования IP-адресации подсетей. На удаленных сторонах могут использоваться одинаковые частные IP-адреса и подсети защищаемых ресурсов.

Для обеспечения такой возможности на каждом узле ViPNet для всех других узлов ViPNet, с которыми у него задана связь, автоматически формируются непересекающиеся виртуальные адреса:

- Для клиентов и координаторов формируется столько же виртуальных адресов, сколько у них есть реальных адресов.
- Для индивидуальных адресов или диапазонов адресов узлов, туннелируемых удаленными координаторами, формируются непересекающиеся виртуальные адреса и диапазоны.

На каждом узле для других узлов и туннелируемых ими устройств формируется свой уникальный набор виртуальных адресов.

Виртуальные адреса узлов не зависят от их реальных адресов и привязаны к уникальным ViPNet-идентификаторам узлов, присвоенным им в управляющем приложении ViPNet Administrator. При изменении IP-адреса удаленного узла ViPNet (что характерно для мобильных компьютеров, устройств и компьютеров с настроенной службой DHCP -client) его виртуальный адрес, единожды созданный на данном узле, не изменится. Это свойство можно использовать в приложениях для надежной аутентификации узла по его виртуальному адресу.

6.2 Адреса видимости

На каждом узле ViPNet известны списки реальных IP-адресов всех узлов ViPNet, с которыми связан данный узел, а также списки IP-адресов туннелируемых координаторами узлов. Узел получает эти адреса разными способами:

1. Списки реальных адресов других клиентов и координаторов передаются на узел в служебных сообщениях из управляющего приложения ViPNet Администратор и за счет работы протокола динамической маршрутизации ViPNet-трафика (см. «Протокол динамической маршрутизации»).

2. Списки реальных адресов узлов, туннелируемых удаленными координаторами, передаются на узел в служебных сообщениях из управляющего приложения ViPNet Администратор.

3. Если зашифрованный трафик приходит от узла, реальный адрес которого не был получен ранее из ViPNet Administrator или за счет протокола динамической

маршрутизации (пп. 1 и 2), то узел регистрирует IP-адрес источника расшифрованного пакета как реальный адрес этого узла.

Как сказано выше, реальным адресам сопоставлены уникальные виртуальные адреса. Приложения на клиентах, координаторах и туннелируемых узлах для взаимодействия с ресурсом на некотором удаленном узле должны использовать адрес видимости — реальный или соответствующий ему виртуальный адрес удаленного узла. Какой адрес (реальный или виртуальный) следует использовать в качестве адреса видимости того или иного узла на данном узле, определяется настройками на данном узле.

Пользователям и администраторам нет необходимости заботиться о том, какой из адресов используется в качестве адреса видимости, и задавать его в приложениях. Приложения, использующие стандартные службы имен (DNS-службы), или мультимедийные приложения, использующие служебные протоколы SCCP, SIP, H.323 и другие (например IP-телефон), автоматически получат правильный IP -адрес другой стороны. В телах пакетов этих протоколов приложениям сообщаются IP-адреса требуемых им ресурсов. ПО ViPNet на клиентах и координаторах обрабатывает пакеты этих протоколов: при их отправке добавляет в инкапсулированные пакеты дополнительную информацию, идентифицирующую узел ViPNet, которому принаждлежит данный IP-адрес. Например, при отправке ответа на DNS-запрос добавляется информация, идентифицирующая IP-адрес защищенного ресурса, имя которого было запрошено. При приеме пакета эта информация позволяет выполнить подмену IP-адреса в теле извлеченного пакета на актуальный адрес видимости требуемого ресурса (адрес видимости на данном узле). Полученный адрес приложения используют для организации разговора с удаленным пользователем, для работы с почтой Exchange, доступа по имени на веб-порталы и другие ресурсы в защищенном режиме.

При обработке входящих расшифрованных пакетов от других узлов в них производится подмена адреса источника на адрес видимости этих узлов на данном узле. В результате приложения на самом узле или его туннелируемых узлах передают ответный трафик на правильный адрес видимости. Такой трафик будет зашифрован и передан на узел назначения.

7. Маршрутизация трафика координаторов с несколькими сетевыми интерфейсами

Координатор ViPNet может иметь произвольное количество физических или виртуальных интерфейсов, подключенных к разным подсетям. Со стороны каждой подсети могут находиться открытые туннелируемые ресурсы.

Для соединения с ресурсами, расположенными за удаленными координаторами, можно настроить использование нескольких альтернативных каналов связи через разные подсети. Для этого нужно задать соответствующие адреса доступа к удаленным координаторам в этих подсетях и, при необходимости, задать метрики, определяющие приоритет их использования.

Приложения, работающие на координаторе или туннелируемых им ресурсах, посылают свои пакеты в адрес удаленных защищаемых ресурсов по их адресам видимости: реальным адресам удаленных узлов (как правило, это частные IP-адреса, выданные в тех локальных сетях, где они находятся) или по соответствующим им автоматически назначенным виртуальным адресам. Операционная система координатора маршрутизирует трафик в соответствии с имеющимися маршрутами для этих адресов.

Однако нет никакой необходимости производить настройки маршрутов для всех многочисленных удаленных подсетей с частными адресами или соответствующих им виртуальных адресов, что было бы особенно сложно, учитывая, что виртуальные адреса выделяются из одной подсети. Драйвер ПО ViPNet самостоятельно обеспечивает маршрутизацию трафика на нужный интерфейс в соответствии с маршрутом, заданным для внешних адресов доступа.

То есть на координаторе достаточно настроить один маршрут по умолчанию и другие необходимые маршруты во внешние маршрутизируемые сети. Это типовой набор настроек для стандартных роутеров.

8.Туннелирование трафика открытых ресурсов на канальном уровне (работа координаторов в режиме L2-шифратора L2-шифратора)

Координаторы типа HW могут быть установлены в режим L2-шифратора (технология туннелирования на канальном уровне L2OverIP). Координаторы в этом режиме устанавливаются на границах нескольких (до 32) удаленных локальных сетей и объединяют их в единую локальную сеть. Узлы в этих локальных сетях взаимодействуют так, как если бы они находились в одном широковещательном домене (без маршрутизации, с прямой видимостью по MAC-адресам).

Координатор в режиме L2-шифратора работает как виртуальный коммутатор, который пересылает поступившие на его L2-адаптер Ethernet-кадры в удаленные сети через аналогичные L2-шифраторы на их границах:

- широковещательные (в частности ARP-запросы) и мультикастовые кадры — во все объединяемые сети;
- юникастовые кадры — в конкретную сеть в соответствии с накопленной таблицей MAC- адресов виртуального коммутатора.

Не имеет значения протокол более высокого уровне (IP или иной) трафика, поступившего на L2-адаптер.

Координатор обрабатывает Ethernet-кадры и не различает IP-пакеты. Поэтому он не может использоваться для туннелирования IP-трафика открытых ресурсов (см. «Туннелирование IP-трафика открытых ресурсов»).

Ethernet-кадр, перехваченный на L2-адаптере, сначала упаковывается в простой IP-пакет с адресом назначения нужного координатора. Широковещательный Ethernet-кадр дублируется в нескольких IP-пакетах с адресами назначения координаторов других локальных сетей. Каждый такой IP-пакет шифруется на ключе связи с соответствующим координатором, инкапсулируется в стандартный ViPNet-пакет и пересылается на нужный координатор через внешний интерфейс. При приеме исходный Ethernet-фрейм извлекается и отправляется в локальную сеть.

Координаторы поддерживают технологию VLAN (802.1Q):

1. Координатор в режиме L2-шифратора может пересылать тегированные кадры в другие сегменты с сохранением тегирования.
2. На L2-адаптере координатора можно создать виртуальные интерфейсы VLAN, которые будут работать через L2-туннель с узлами в удаленных сегментах с учетом их нахождения в VLAN.

Можно увеличить производительность L2-канала между локальными сетями за счет подключения нескольких координаторов к внешнему коммутатору через разные порты по технологии EtherChannel. Испытания такого кластера из трех координаторов HW2000 показали производительность 10 Гбит/с (прямо-пропорциональное числу координаторов увеличение производительности).

Практическая часть

1. Установить программу VipNet Custom
2. Настроить Часть VipNet Coordinator
3. Настроить Часть VipNet Client
4. Установить VPN соединение между двумя машинами
5. Прослушать трафик между машинами связанными VPN соединением и убедиться что трафик действительно шифрован

Работа с литературой:

Рекомендуемые источники информации (№ источника)

Основная	Дополнительная	Методическая	Интернет-ресурсы
1-2	1-2	1-2	1-4

Оценочные средства: отчет к лабораторной работе (См.: Фонд оценочных средств)

Лабораторная работа № 3
«Принципы защиты отдельных сервисов с помощью туннелирования трафика (ZeBeDee)»

Форма проведения: **лабораторная работа**

Цель работы:

Ознакомиться с принципами защиты отдельных сервисов с помощью туннелирования трафика (ZeBeDee)

Теоретические сведения.

Открытая внешняя среда передачи информации включает как каналы скоростной передачи данных, в качестве которой используется сеть Интернет, так и более медленные общедоступные каналы связи, в качестве которых обычно применяются каналы телефонной сети. Эффективность виртуальной частной сети VPN определяется степенью защищенности информации, циркулирующей по открытым каналам связи. Для безопасной передачи данных через открытые сети широко используют инкапсуляцию и туннелирование. С помощью методики туннелирования пакеты данных передаются через общедоступную сеть, как по обычному двухточечному соединению. Между каждой парой «отправитель — получатель данных» устанавливается своеобразный туннель — логическое соединение, позволяющее инкапсулировать данные одного протокола в пакеты другого.

Суть туннелирования состоит в том, чтобы инкапсулировать, т. е. «упаковать», передаваемую порцию данных, вместе со служебными полями, в новый «конверт». При этом пакет протокола более низкого уровня помещается в поле данных пакета протокола более высокого или такого же уровня. Следует отметить, что туннелирование само по себе не защищает данные от НСД или искажения, но благодаря туннелированию появляется возможность полной криптографической защиты инкапсулируемых исходных пакетов. Чтобы обеспечить конфиденциальность передаваемых данных, отправитель шифрует исходные пакеты, упаковывает их во внешний пакет с новым IP-заголовком и отправляет по транзитной сети (рис. 1)

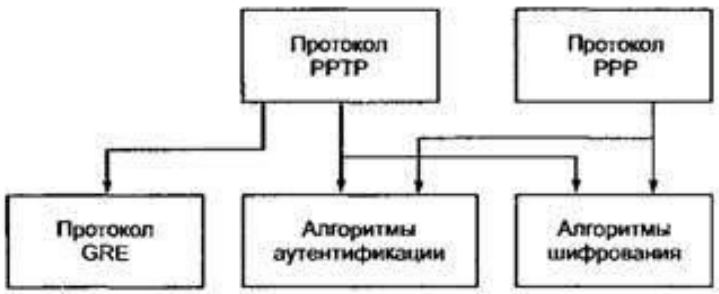


Рис. 1. Пример пакета, подготовленного для туннелирования

Особенность технологии туннелирования в том, что она позволяет зашифровывать исходный пакет целиком, вместе с заголовком, а не только его поле данных. Это важно,

поскольку некоторые поля заголовка содержат информацию , которая может быть использована злоумышленником. В частности, из заголовка исходного пакета можно извлечь сведения о внутренней структуре сети — данные о количестве подсетей и узлов и их IP-адресах. Злоумышленник может использовать такую информацию при организации атак на корпоративную сеть. Исходный пакет с зашифрованным заголовком не может быть использован для организации транспортировки по сети. Поэтому для защиты исходного пакета применяют его инкапсуляцию и туннелирование. Исходный пакет зашифровывают полностью, вместе с заголовком, и затем этот зашифрованный пакет помещают в другой внешний пакет с открытым заголовком. Для транспортировки данных по открытой сети используются открытые поля заголовка внешнего пакета.

По прибытии в конечную точку защищенного канала из внешнего пакета извлекают внутренний исходный пакет, расшифровывают его и используют его восстановленный заголовок для дальнейшей передачи по внутренней сети (рис. 2).

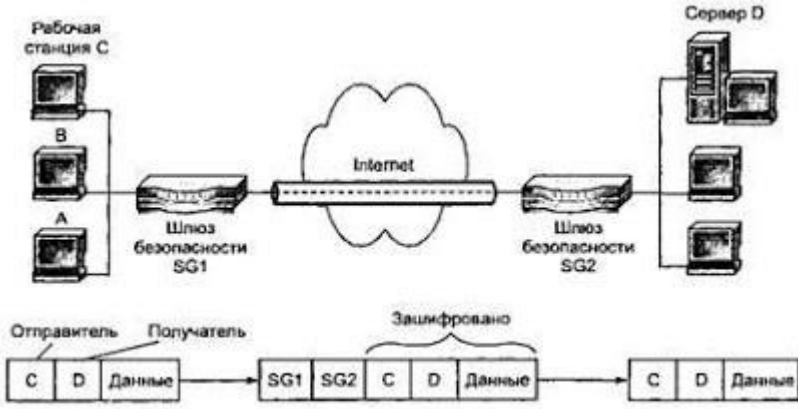


Рис. 2. Схема виртуального защищенного тунеля

Туннелирование может быть использовано для защиты не только конфиденциальности содержимого пакета, но и его целостности и аутентичности, при этом электронную цифровую подпись можно распространить на все поля пакета.

В дополнение к сокрытию сетевой структуры между двумя точками, туннелирование может также предотвратить возможный конфликт адресов между двумя локальными сетями. При создании локальной сети, не связанной с Internet, компания может использовать любые IP-адреса для своих сетевых устройств и компьютеров. При объединении ранее изолированных сетей эти адреса могут начать конфликтовать друг с другом и с адресами, которые уже используются в Internet. Инкапсуляция пакетов решает эту проблему, поскольку позволяет скрыть первоначальные адреса и добавить новые, уникальные в пространстве IP-адресов Internet, которые затем используются для пересылки данных по разделяемым сетям. Сюда же входит задача настройки IP-адреса и других параметров для мобильных пользователей, подключающихся к локальной сети.

Применение
Механизм туннелирования широко применяется в различных протоколах формирования защищенного канала. Обычно туннель создается только на участке открытой сети, где существует угроза нарушения конфиденциальности и целостности данных, например между точкой входа в открытый Интернет и точкой входа в корпоративную сеть. При этом для внешних пакетов используются адреса пограничных маршрутизаторов, установленных в этих двух точках, а внутренние адреса конечных узлов содержатся во внутренних исходных пакетах в защищенном виде. Следует отметить, что сам механизм

туннелирования не зависит от того, с какой целью применяется туннелирование. Туннелирование может применяться не только для обеспечения конфиденциальности и целостности всей передаваемой порции данных, но и для организации перехода между сетями с разными протоколами (например, IPv4 и IPv6). Туннелирование позволяет организовать передачу пакетов одного протокола в логической среде, использующей другой протокол. В результате появляется возможность решить проблемы взаимодействия нескольких разнотипных сетей, начиная с необходимости обеспечения целостности и конфиденциальности передаваемых данных и заканчивая преодолением несоответствий внешних протоколов или схем адресации.

Реализация
Реализацию механизма туннелирования можно представить как результат работы протоколов трех типов: протокола-«пассажира», несущего протокола и протокола туннелирования. Например, в качестве протокола-«пассажира» может быть использован транспортный протокол IPX, переносящий данные в локальных сетях филиалов одного предприятия. Наиболее распространенным вариантом несущего протокола является протокол IP сети Интернет. В качестве протоколов туннелирования могут быть использованы протоколы канального уровня PPTP и L2TP, а также протокол сетевого уровня IPSec. Благодаря туннелированию становится возможным сокрытие инфраструктуры Internet от VPN-приложений.

Туннели VPN могут создаваться для различных типов конечных пользователей — либо это локальная сеть LAN (local area network) со шлюзом безопасности, либо отдельные компьютеры удаленных и мобильных пользователей. Для создания виртуальной частной сети крупного предприятия нужныVPN-шлюзы, VPN-серверы и VPN-клиенты. VPN-шлюзы целесообразно использовать для защиты локальных сетей предприятия, VPN-серверы и VPN-клиенты используют для организации защищенных соединений удаленных и мобильных пользователей с корпоративной сетью через Интернет.

Свободно распространяемый инструмент Zebedee предназначен для защищенного туннелирования протоколов TCP и UDP через Internet. К его основным функциям относятся шифрование, аутентификация и сжатие данных. В качестве специализированной программы туннелирования Zebedee может предложить ряд возможностей, которые нельзя найти в других аналогичных решениях, например в SSH. Программа может работать под управлением как Linux, так и Windows.

Использование туннелей TCP для защищенной коммуникации с другими системами пользователи SSH воспринимают как удобное дополнение к сеансам Secure Shell. Эта технология может помочь администраторам, когда речь идет о выполнении задач по обслуживанию удаленной сети через Internet посредством telnet, HTTP или, к примеру, удаленной программы управления VNC. Такое туннелирование отдельных протоколов, хотя и не слишком удобно, но предлагает достаточные возможности для доступа. В результате становится ненужной организация более дорогих соединений между локальными сетями или виртуальных частных сетей (Virtual Private Network, VPN).

Этот свободно распространяемый инструмент предназначен исключительно для организации туннелей и поэтому не может стать альтернативой таким громоздким программным средствам, как SSH, однако он отличается большой функциональностью и необходимой гибкостью.

Один из интересных аспектов Zebedee состоит в том, что она может устанавливать туннели не только между портами TCP, но и между портами UDP. Таким образом появляются дополнительные возможности, в том числе создание туннелей SNMP (порт UDP 161). Как и в случае с SSH, все туннели (включая UDP) проходят по одному соединению TCP, которое, в отличие от SSH, по умолчанию использует не порт TCP 22, а порт TCP 11965. С его помощью Zebedee может отправить по туннелю и саму себя,

благодаря чему пользователи, которые хотели бы сохранить существующее соединение SSH, смогут передать Zebedee по туннелю SSH и в дальнейшем работать с UDP.

Еще один положительный аспект программы Zebedee, которую мы тестировали в среде Windows, не столь очевиден: один файл *.exe служит и сервером, и клиентской программой, а потому выполняется как из командной строки, так и инсталлируется в виде службы NT. Следовательно, у Zebedee не только серверный, но и клиентский компонент может исполняться как служба NT. Этот рабочий режим обеспечивает высокую готовность и стабильность туннелей, особенно когда они используются не индивидуально, а предоставляются другим компьютерам или сетевым устройствам в качестве коммуникационной услуги. Поскольку имя службы NT также назначается произвольно, на одном и том же компьютере параллельно могут работать несколько экземпляров служб Zebedee для различных прикладных целей (например, для серверной и клиентской служб).

При этом построенные с помощью Zebedee туннели обладают большей надежностью, чем, к примеру, туннели SSH, поскольку последние создаются каждый раз в рамках одного фиксированного сеанса. Туннели Zebedee состоят из последовательности отдельных коротких соединений и создаются в зависимости от потребности в них, благодаря чему туннельное соединение выдерживает длительные физические разрывы. Соединение Zebedee «не смутит» даже смена IP-адреса системы-получателя: определение адреса по доменному имени происходит при установлении каждого отдельного соединения. Поэтому Zebedee великолепно подходит для организации длительных по времени туннелей в сети, доступ к которым производится через Internet посредством, к примеру, DSL с фиксированной ставкой и динамической DNS, причем их общедоступный IP-адрес меняется максимум через 24 ч.

Вариант Zebedee для Windows поставляется в виде удобной программы установки. В соответствующий каталог инсталлируется собственно продукт, файл подсказки в формате HTML длиной почти 50 страниц, а также некоторые демонстрационные конфигурации. Программа адаптируется в соответствии с индивидуальными требованиями путем задания различных параметров в командной строке или простого изменения конфигурационного файла в формате ASCII с расширением ***.zbd**. Этот тип файлов при инсталляции автоматически ассоциируется с Zebedee, благодаря чему туннельные соединения могут организовываться непосредственно после вызова соответствующего конфигурационного файла. Мобильным пользователям, которым часто приходится работать за чужими компьютерами, интересно будет узнать, что инсталляция программы в описанном виде вовсе не обязательна: в крайнем случае достаточно дискеты с ***.exe** и, при необходимости, индивидуальных конфигурационных файлов. Таким образом практически отовсюду можно легко построить надежные туннельные соединения, например, с собственным офисом.

Как и SSH, Zebedee использует по умолчанию шифрование и сжатие данных в туннелях. Название программы — библейское имя Зеведей — образовано, по утверждению производителя, от первых букв трех лежащих в ее основе технологий: сжатие — Zlib, шифрование — Blowfish и соглашение о ключах — Diffie-Hellman. Хотя аутентификация клиентской и серверной сторон в Zebedee необязательна, но она возможна в обоих направлениях с помощью пар открытых/личных ключей и настоятельно рекомендуется. Пары ключей генерируются программой на месте, однако автоматическое распределение соответствующих открытых ключей не реализовано. Для этого пользователю придется воспользоваться другими средствами передачи — дискетой или электронной почтой. Ключи хранятся в отдельных файлах формата ASCII, которые — так же как и пути к ним — могут быть ассоциированы с различными конфигурациями.

Основная концепция построения туннелей в случае Zebedee и SSH практически одинакова: клиент и сервер образуют конечные пункты для защищенного туннельного соединения, однако в качестве пунктов назначения при передаче данных могут быть

указаны и другие IP-устройства в серверной сети. Другие устройства в сети отправителя также могут использовать установленные клиентом туннельные соединения. В обоих случаях накладываются определенные ограничения. Конечно же, Zebedee поддерживает многократные соединения с различными адресами в серверной сети посредством одного-единственного запроса. Синтаксис позволяет даже снабжать определения туннелей списками портов, разделенных запятыми, например:

8080, 2000-2100:<Целевой хост>:80, 3000-3100

Порты TCP и UDP можно объединять в смешанные списки при помощи соответствующих ключей . Особенностью Zebedee является возможность освобождения входного порта туннеля и тем самым предоставления его программе. Пользователю нет необходимости самостоятельно проверять, заняты ли локальные порты (например, при помощи команды операционной системы netstat -an). Использовать эту возможность, конечно, можно, но только с такими приложениями , как telnet, которые могут адресовать передачу данных на любые порты. Реальный смысл этот вариант имеет в комбинации с возможностью связать Zebedee с программным вызовом. Синтаксис позволяет передать локальный порт приложению через переменную в качестве параметра. Так, к примеру, вызов

zebedee -f "telnet localhost %d" <Целевой хост>

запускает сначала Zebedee, а потом telnet с выбранным программой локальным портом. После завершения интегрированного приложения останавливается и выполнение Zebedee. При работе на чужих компьютерах такой «туннель по требованию» может оказаться очень полезным, поскольку пользователю не придется заботиться о диспозиции туннельного соединения.

Абсолютно иначе, по сравнению с SSH, решается задача обратных туннелей. SSH использует существующие уже сеансы от клиента к серверу, чтобы при необходимости одновременно создать заранее определенные туннели в обратном направлении. В случае Zebedee это невозможно. Для обратных туннелей клиенты и серверы Zebedee придется перезапустить в специальных рабочих режимах, именуемых «клиентский хост» и, соответственно, «режим прослушивания». При этом коммуникационный порт 11965 открывает не сервер, а клиент; сервер же пытается «дозвониться» до клиента. После установления соединения определенные таким образом туннели функционируют в обычном режиме.

Zebedee в последней «стабильной версии» 2.4.1 предоставляет весьма ограниченные возможности работы с обратными туннелями: клиент при запуске сервера должен быть готовым к приему, что в любом случае делает необходимой синхронизацию этих процессов «по внешнему каналу» (например, предварительное согласование момента включения или непосредственная договоренность по телефону). В разрабатываемой версии 2.5.2 обратным туннелям уделено больше внимания, судя по конфигурируемым механизмам повтора и возможности задания тайм-аутов. Однако тем, кому приходится постоянно пользоваться обратными туннелями, нельзя полностью полагаться на данные технологии. Как минимум, на стороне сервера можно посоветовать вместо службы NT работать с бесконечным командным файлом, как это уже предлагалось редакцией LANline в связи с туннелями SSH.

Такая программа, как Zebedee, обеспечивает хороший базис для построения туннелей, однако каждый пользователь должен решить сам, какие приложения и, в определенных случаях, с помощью каких приемов можно успешно туннелировать. Zebedee предусматривает специальную поддержку для *ftp,* однако об автономном решении, предлагаемом, например, SSH вместе с ее графическим клиентом Windows, речи не идет. Для создания туннеля NetBIOS/SMB (порт TCP 139) Zebedee предусматривает элегантную возможность конфигурации, благодаря чему становится возможным беспроблемный удаленный доступ к разделяемым ресурсам Windows (дополнительную информацию по этому вопросу см. в архиве электронной почты сайта Zebedee).

В заключение следует указать на то, что именно свободный программный инструмент, каким является Zebedee, открывает такие возможности его применения в корпоративных сетях, о которых не сразу задумываются в случае дорогих продуктов. Так, Zebedee благодаря механизмам сжатия можно применять для передачи по туннелям приложений с высокими требованиями к пропускной способности. В качестве примера можно привести задания на печать на порт очереди принтеров (часто 9100). Zebedee может оказаться полезным средством для организации защищенных от прослушивания соединений в пределах предприятия или при использовании внутренних брандмауэров.

1. Установить программу ZBD на клиентской машине и на сервере
2. Настроить клиентскую и серверную части.
3. Добиться соединения между машинами
4. Прослушать трафик между машинами и убедиться что трафик действительно шифрован.

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы
1-2	1-2	1-2	1-4

Оценочные средства: отчет к лабораторной работе (См.: Фонд оценочных средств)

Лабораторная работа №4
«Система защиты корпоративной информации «Secret Disk»»

Форма проведения: **лабораторная работа Цель работы:**

Изучить основные принципы системы защиты корпоративной информации «Secret Disk».

Теоретические сведения.

СИСТЕМА ЗАЩИТЫ КОРПОРАТИВНОЙ ИНФОРМАЦИИ "SECRET DISK SERVER"

Назначение

Secret Disk Server служит для защиты конфиденциальной информации, корпоративных баз данных. Система предназначена для работы в Windows NT 4.0 Server / Workstation, поддерживает работу с IDE и SCSI-дисками, со всеми типами RAID-массивов. Защищаемые разделы могут содержать файловую систему FAT или NTFS. Система не только надежно защищает конфиденциальные данные, но и скрывает их наличие.

Принцип работы

Защита информации осуществляется путем "прозрачного" (на лету) шифрования содержимого разделов жесткого диска (логических дисков).
При установке Secret Disk Server выбранные логические диски зашифровываются. Права доступа к ним для пользователей сети устанавливаются средствами Windows NT. Шифрование осуществляется программно, системным драйвером ядра (kernel-mode driver).

Шифрование

Помимо встроенного алгоритма преобразования данных с длиной ключа 128 бит, Secret Disk Server позволяет подключать внешние модули криптографической защиты, например, входящий в Windows RC-4 или эмулятор известной платы "Криптон", реализующей мощнейший российский алгоритм шифрования ГОСТ 28147-89 с длиной

ключа 256 бит.
Скорость шифрования очень высока, поэтому мало кто сможет заметить небольшое замедление при работе.

Ключи шифрования

Ключи шифрования вводятся в драйвер Secret Disk Server перед началом работы с защищенными разделами (или при загрузке сервера). Для этого используются микропроцессорные карточки (смарткарты), защищенные PIN-кодом. Не зная код, воспользоваться карточкой нельзя. Три попытки ввода неправильного кода заблокируют карту.
При работе сервера смарткарта не нужна, и ее можно спрятать в надежное место.
Во время работы системы ключи шифрования хранятся в оперативной памяти сервера и никогда не попадают на диск в файл подкачки (swap file).

Генерация ключей шифрования

Генерация PIN-кодов и ключей шифрования производится самим пользователем. При генерации используется последовательность случайных чисел, формируемая по траектории движения мыши и временным характеристикам нажатия произвольных клавиш.

Открытый интерфейс

Secret Disk Server имеет открытый интерфейс для подачи сигнала "тревога" и позволяет подключать различные датчики и устройства контроля доступа в помещение (датчики открывания дверей, окон, движения, изменения объема, электронные и кодовые замки).
При подключении защищенных дисков возможен автоматический запуск необходимых программ и сервисов, перечисленных в конфигурационном файле.

Утечка информации может стать для компании причиной многих бед. Как защититься от внезапно нагрянувших "гостей"? С помощью системы "прозрачного" шифрования данных Secret Disk Server (старое название SecureNT).

Многие считают, что их корпоративные базы данных надежно защищены паролем. Но пароль лишь ограничивает доступ. Чтобы открыть информацию достаточно переставить диски на другой компьютер.
Самым слабым звеном любой системы являются люди. Особенно в критических ситуациях. Знать о Secret Disk Server могут лишь 2-3 человека. Остальные даже и не заметят каких-либо изменений в работе.

Secret Disk Server автоматически зашифровывает данные при записи на сервер и расшифровывает их при чтении. Ключ шифрования вводится при загрузке сервера со смарткарты, защищенной PIN-кодом. В процессе работы смарткарта не требуется и ее можно убрать в надежное место.

Если "унесли" сервер...

После перезагрузки сервера без предъявления смарткарты или попытки чтения дисков на другом компьютере, защищенные разделы будут "видны" как неформатированные области, прочитать которые нельзя. При возникновении опасности можно мгновенно "уничтожить" информацию, сделав защищенные разделы "невидимыми". Для блокирования информации серверу подается сигнал "тревога":

- с клавиатуры любой станции сети от "красной кнопки" (спрятанной под столом);
- от охранной сигнализации (датчиков открывания дверей, окон, движения и пр.);
- от кодового замка (при входе в помещение под принуждением);
- Назначение Secret Disk Server служит для защиты конфиденциальной информации, корпоративных баз данных. Система предназначена для работы в Windows NT 4.0 Server / Workstation, Windows 2000, поддерживает работу с IDE и SCSI-дисками, со всеми типами RAID-массивов. Защищаемые разделы могут

содержать файловую систему FAT или NTFS. Система не только надежно защищает конфиденциальные данные, но и скрывает их наличие. Принцип работы

Защита информации осуществляется путем "прозрачного" (на лету) шифрования содержимого разделов жесткого диска (логических дисков). При установке Secret Disk Server выбранные логические диски зашифровываются. Права доступа к ним для пользователей сети устанавливаются средствами Windows NT. Шифрование осуществляется программно, системным драйвером ядра (kernel-mode driver).

1. Установить программу на клиентской машине и на сервере
2. Настроить клиентскую и серверную части.
3. Добиться соединения между машинами
4. Прослушать трафик между машинами и убедиться что трафик действительно шифрован.

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы
1-2	1-2	1-2	1-4

Оценочные средства: отчет к лабораторной работе (См.: Фонд оценочных средств)

Лабораторная работа № 5
«Использование протокола IPSec для защиты сетей»

Форма проведения: **лабораторная работа Цель работы:**

Ознакомиться с возможностями использования протокола IPSec для защиты сетей.

Теоретические сведения

Как правило, протокол IP Security (IPsec) используется при построении каналов VPN, однако с его помощью можно существенно повысить и уровень защищенности сети. Применение IPsec позволяет решить три типичные проблемы, а именно воспрепятствовать распространению «червей», защитить серверы сети и изолировать домен. Причем ни в одном из случаев не требуется использовать шифрование, существенно снижающее производительность систем. Рассмотрим каждое из этих решений.

IPSec против «червей»

Конечно, лучший способ борьбы с «червями» состоит в том, чтобы не допускать их появления. Но, увы, не все осознают потенциальные угрозы, с которыми связаны использование электронной почты и навигация в Web. На данный момент, к сожалению, надо признать, что от «червей» и других видов вредоносных программ сегодня никуда не деться. Как же можно в данной ситуации снизить риск поражения системы вредоносным кодом? Путей борьбы с подобными программами три: предотвратить возможность установки, не допустить запуска и исключить для таких программ возможность установки каких-либо сетевых соединений.

В ряде случаев единственная возможность одолеть вредоносные программы состоит в том, чтобы исключить для них возможность установки соединений. Используя политики IPsec, можно ограничить для компьютера типы передаваемого и принимаемого трафика. В качестве эффективных базовых фильтров пакетов на отдельных компьютерах можно использовать правила с описаниями фильтров, которые будут просто блокировать или пропускать тот или иной трафик (без применения каких либо функций безопасности IPsec security associations, таких как аутентификация или шифрование трафика). Эти

правила могут быть переданы на компьютеры с помощью механизмов групповых политик , что, в свою очередь, поможет воспрепятствовать распространению вредоносного трафика по сети.

Выбор тех или иных политик IPsec определяется типом используемой операционной системы. В Windows 2003 Server и Windows XP имеется встроенный межсетевой экран Windows Firewall, который обеспечивает более эффективную блокировку входящего трафика, чем применение IPsec. Соответственно, если используются эти системы и Windows Firewall, то политики IPsec следует применять только для блокировки исходящего трафика. В операционной системе Windows 2000 межсетевой экран отсутствует, поэтому для компьютеров, работающих под управлением этой системы, можно блокировать входящий и исходящий трафик с помощью политик IPsec.

Рассмотрим в качестве примера «червя» Slammer. Путем распространения по сети сообщений через порт UDP номер 1434 этот вирус обнаруживает в сети компьютеры с запущенными на них Microsoft SQL Server или Microsoft SQL Server Desktop Engine (MSDE). Компания Microsoft выпустила соответствующее исправление, но, чтобы установить его на все компьютеры, потребуется некоторое время. Существует превосходное решение, позволяющее сократить время, необходимое для принятия первоочередных мер защиты. Оно заключается в том, чтобы с помощью групповых политик распространить на компьютеры политики IPsec, которые обеспечат блокировку входящего трафика через уязвимый порт. Безусловно, это блокирует и входящий трафик систем с SQL Server, поэтому после установки исправлений на уязвимые системы данную политику для них следует отменить.

Для того чтобы предотвратить заражение компьютера «червем» Slammer, нужно назначить политику, блокирующую весь трафик, поступающий на IP-адрес данного компьютера через UDP-порт назначения 1434. Соответствующая политика выглядит следующим образом.

- В списке фильтров должен быть задан фильтр: от любой адрес:любой порт на адрес компьютера:порт 1434/udp.
- Действие фильтра: блокировка.
- Правило: связать список с действием; для всех сетевых интерфейсов; без туннеля; метод аутентификации — любой (в данном случае не имеет значения, какой метод используется для аутентификации, поскольку в этом блокирующем фильтре функции безопасности для IPsec не заданы).

Для того чтобы создать политику, сначала следует запустить консоль управления IPsec на том компьютере, который нужно защитить. Для Windows 2003, Windows XP и Windows 2000 процедура одинакова.

1. Дважды щелкните мышью на значке «Локальная политика безопасности» (Local Security Policy) в папке «Администрирование» (Administrative Tools).
2. Выберите раздел «Политики безопасности IP на локальном компьютере» (IP Security Policies on Local Computer).

Создайте список фильтров:

1. Щелкните правой кнопкой мыши в правой половине окна «Локальные настройки безопасности» (Local Security Settings) и выберите в контекстном меню пункт «Управление списками IP-фильтра и действиями фильтра» (Manage IP filter lists and filter actions).
2. На закладке «Управление списками фильтров IP» (Manage IP Filter Lists) нажмите кнопку «Добавить» (Add).
3. Введите в поле имени название списка: Slammer filter list.
4. В появившемся стартовом окне мастера фильтров IP нажмите кнопку «Добавить», а затем кнопку «Далее» (Next).
5. В качестве источника выберите «Любой IP-адрес» (Any IP Address).

6. В качестве назначения выберите «Мой IP-адрес» (My IP Address).
7. В качестве протокола выберите UDP.
8. Выберите пункт «Пакеты на этот порт» (To this port) и введите в поле значение 1434.
9. Для завершения работы мастера нажмите кнопку «Готово» (Finish).
10. Щелкните OK.

Теперь необходимо создать действие фильтра (если в системе уже создано действие с названием «Блокировка» (Block), этот пункт следует пропустить):

1. В диалоговом окне «Управление списками IP-фильтра и действиями фильтра» (Manage IP filter lists and filter actions) перейдите на закладку «Управление действиями фильтра» (Manage Filter Actions) и нажмите кнопку «Добавить». В появившемся стартовом окне мастера настройки действий фильтров IPsec нажмите кнопку «Далее».
2. В поле имени введите Block.
3. В окне настройки общих параметров действия фильтра выберите «Блокировать» (Block).
4. Для завершения работы мастера нажмите кнопку «Готово»
5. Для того чтобы завершить процедуру настройки списка и действий фильтров, нажмите кнопку «Закрыть» (Close).

Затем нужно создать политику IPsec:

1. Щелкните правой кнопкой мыши в правой половине окна «Локальные настройки безопасности», выберите из контекстного меню пункт «Создать политику безопасности IP» (Create IP Security Policy) и в появившемся окне мастера политики IP-безопасности нажмите кнопку «Далее».
2. Введите в поле имени Slammer filter.
3. Снимите галочку с пункта «Использовать правило по умолчанию» (Activate the default response rule) и нажмите «Далее».
4. Оставьте пункт «Изменить свойства» (Edit properties) выбранным и нажмите кнопку «Готово» для завершения работы мастера.

Теперь нужно добавить к созданной политике правило:

1. В появившемся диалоговом окне свойств политики нажмите кнопку «Добавить», затем кнопку «Далее».
2. В трех следующих окнах оставьте все настройки без изменений.
3. Из перечня списков фильтров выберите список Slammer filter.
4. Из списка действий фильтров выберите Block.
5. Для завершения работы мастера нажмите кнопку «Готово», после чего закройте диалоговое окно свойств правила, нажав OK.
6. Закройте диалоговое окно свойств политики с помощью кнопки «Закрыть».

И наконец, необходимо назначить выбранную политику: щелкнуть правой кнопкой на значке политики Slammer filter и выбрать пункт «Назначить» (Assign).

Создание политики IPsec с помощью сценария

Политики IPSec можно создавать и с помощью командной строки, что очень удобно, поскольку описанные процедуры могут выполняться из соответствующего сценария. В Windows 2000 для этого используется утилита ipsecpol.exe из пакета Microsoft Windows 2000 Resource Kit; в Windows XP применяется утилита ipseccmd.exe из пакета Windows Support Tools for Microsoft Windows XP; что же касается систем семейства Windows 2003, то необходимый программный инструмент, а именно утилита Netsh Ipsec, входит в состав этих операционных систем. Для того чтобы применить политику Slammer filter на системе с Windows XP, можно воспользоваться следующей командой:

ipseccmd -w REG -p «Block UDP 1434 Filter»

-r «Block Inbound UDP 1434 Rule»

*-f *=0:1434:UDP -n BLOCK -x*

Важно строго следовать приведенному синтаксису написания букв, поскольку утилиты ipsecpol.exe и ipseccmd.exe чувствительны к регистру. Также следует помнить, что рассматриваемая командная строка представляет собой одну команду, поэтому вводиться она должна одной строкой.

С помощью показанной выше команды создается и назначается статическая политика под названием Block UDP 1434 Filter, имеющая единственное правило с названием Block Inbound UDP 1434 Rule, в котором содержится созданный нами список фильтров со ссылкой на действие фильтра Block. Статические политики записываются в реестр и сохраняются после перезагрузки системы. Нужно иметь в виду, что политика не будет применена до следующего запуска или перезапуска агента политики IPsec, поэтому если необходимо, чтобы она сразу же вступила в действие, в сценарий следует включить процедуру остановки и повторного запуска службы policyagent. Если же политика была создана через графический интерфейс, то она вступает в силу немедленно.

В том случае когда компьютер уже заражен вирусом Slammer, можно с помощью другого правила IPsec лишить его возможности заражать остальные компьютеры в сети, блокируя исходящие с этого компьютера соединения через порт UDP 1434. Соответствующая политика выглядит следующим образом.

•Список с одним фильтром: *от адрес компьютера:любой порт на любой адрес:порт 1434/udp.*

•Действие фильтра: блокировка.

• Правило: связать список с действием; для всех сетевых интерфейсов; без туннеля; метод аутентификации — любой.

Прошу обратить внимание на одно отличие: в рассмотренном ранее правиле (для входящего трафика) проверялся трафик *от любого адреса:любого порта на адрес компьютера:порт 1434/udp*, здесь же создается правило для фильтрации исходящего трафика, то есть *от адреса компьютера: через любой порт на любой адрес:порт 1434/udp*. С помощью данного правила будет блокирован любой исходящий трафик через порты UDP 1434 остальных компьютеров сети. Для того чтобы создать такое правило в сценарии и добавить его в ту же политику, в которую было добавлено предыдущее правило, используется следующая команда:

ipseccmd -w REG -p «Block UDP 1434 Filter»

-r «Block Outbound UDP 1434 Rule»

-f 0=:1434:UDP -n BLOCK*

В рассмотренной ранее команде применялся ключ -x, означающий создание новой политики. Во втором примере этот ключ пропущен, поскольку здесь мы добавляем к существующей политике новое правило. Также обратите внимание, что в той части рассматриваемой команды, которая касается списка фильтров, символы «0» и «*» поменялись местами. Это связано с тем, что направление действия фильтра изменилось.

С помощью утилит командной строки можно применять и динамические политики, которые действуют только до тех пор, пока система включена (при перезапуске службы policyagent или перезагрузке компьютера они теряются). Динамические политики могут пригодиться в тех случаях, когда заранее известно, что они будут применяться непродолжительное время, а для отмены их действия планируется использовать перезагрузку. Динамическая политика, выполняющая те же функции, что и только что рассмотренная статическая, может быть создана с помощью двух приведенных ниже команд:

ipseccmd -f[=0:1434:UDP]*

ipseccmd -f[0=:1434:UDP]*

Описание фильтра заключено в квадратные скобки — это говорит о том, что отфильтрованный трафик будет блокироваться.

До сих пор мы рассматривали примеры использования IPsec для блокирования трафика в обоих направлениях относительно известных нам уязвимых портов. При создании политик IPsec можно устанавливать более жесткие ограничения, блокируя весь трафик в обоих направлениях и создавая правила, разрешающие только определенный трафик по некоторым портам. Нужно продумать, какой именно тип трафика следует разрешить, тщательно спланировать необходимые мероприятия, провести расширенное тестирование вносимых изменений и лишь после этого внедрять их в действующую инфраструктуру.

IPsec на защите серверов

Одним из характерных примеров применения политик типа «запретить все, кроме» является защита серверов. Действительно, зачем, например, Web-серверу принимать через свой интерфейс, подключенный к Internet, что-то еще, кроме трафика Web? С помощью политики IPsec можно построить элементарный фильтр пакетов, который будет отбрасывать все поступающие данные, за исключением тех, которые необходимы для полноценного выполнения функций сервера. В рассматриваемом примере с Web-сервером может быть блокирован весь трафик, за исключением соединений через порт 80 протокола TCP (а также через порт TCP 443 в тех случаях, когда необходимо просматривать страницы с помощью протокола, защищенного HTTP (HTTPS)).

Политика защиты серверов также может использоваться для экономии времени при тестировании и распространении исправлений. Когда в операционной системе обнаруживается очередное слабое место, можно применить политику, запрещающую доступ к уязвимой службе, что позволит выиграть дополнительное время для тестирования выпущенных исправлений.

Рассмотрим пример построения политики для Web-сервера. Эта политика содержит два правила.

Правило 1

- Один фильтр в списке: от любой адрес:любой порт на адрес компьютера:любой порт.
- Действие фильтра: блокировать.
- Правило: связать список с действием; для всех сетевых интерфейсов; без туннеля; метод аутентификации — любой.

Правило 2

- Два фильтра в списке: < любой адрес >:< любой порт > на < адрес компьютера >:< порт 80/tcp> и < любой адрес >:< любой порт > на < адрес компьютера >:< порт 443/tcp>.
- Действие фильтра: разрешить.
- Правило: связать список с действием; для всех сетевых интерфейсов; без туннеля; метод аутентификации — любой.

Чтобы создать данную политику через сценарий, используется такая последовательность команд:

ipseccmd -w REG

-p «Web traffic packet filter»

-r «Block everything»

-f *+0 -n BLOCK -x

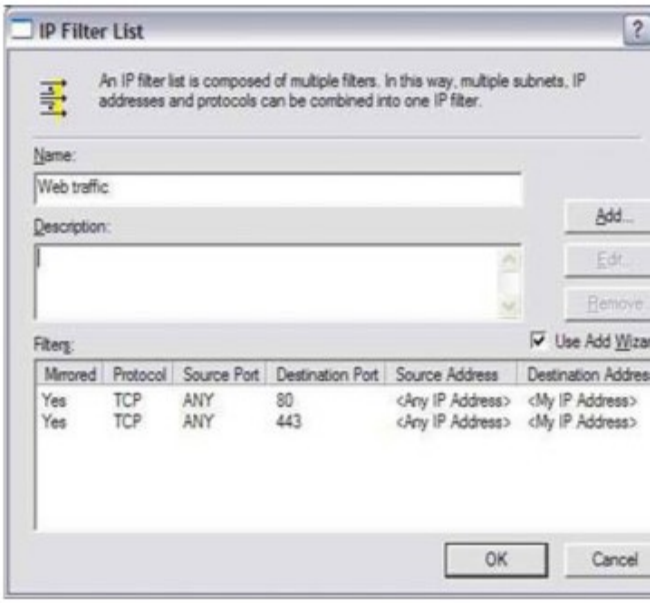
ipseccmd -w REG

-p «Web traffic packet filter»

-r «Permit web traffic»

-f *+0:80:TCP -f *+0:443:TCP

-n PASS



Экран 1. Список фильтров пакетов для Web-трафика

Обратите внимание на то, что в данных примерах между описаниями комбинаций «IP адрес:порт:протокол» источника и получателя вместо знака равенства (=) используется знак плюс (+). Это указывает агенту политики на то, что создаются «зеркальные» правила, разрешающие Web-серверу трафик данного типа. В противном случае нужно было бы построить два отдельных правила, разрешающие исходящий трафик от Web-сервера через порты TCP 80 и 443. Если эти правила создаются через графический интерфейс, то они автоматически будут считаться зеркальными. На экране 1 показано, как выглядит список фильтров для Web-сервера в графическом интерфейсе. На экране 2 представлена политика фильтрации пакетов Web, содержащая два правила, одно из которых блокирует весь трафик, а другое разрешает трафик Web.

Экран 2. Политика фильтра пакетов для Web-трафика

Можно ли выполнить эту задачу с помощью встроенного в систему межсетевого экрана? Безусловно, можно, и для системы Windows Server 2003 я бы выбрал именно такое решение. Но если мы имеем дело с Windows 2000 Server, то использование механизмов фильтрации пакетов с помощью IPsec помогает весьма эффективно сузить зону, которая является потенциально опасной для различных видов атак. Сначала проводится анализ тех функций, которые выполняет каждый из серверов предприятия. После этого, с учетом выполняемых серверами функций, для них разрабатываются политики IPsec. Затем, если сгруппировать учетные записи серверов в организационные подразделения (OU) в соответствии с решаемыми задачами, то распространение на них созданных политик может быть реализовано через механизмы групповой политики. С помощью этой простой методики ограничения поступающего на сервер трафика можно значительно повысить степень защищенности информационной инфраструктуры предприятия.

Изолирование доменов

Обычно администратор располагает данными о том, какие пользователи могут быть аутентифицированы контроллером домена (DC) при попытках обращения к сетевым ресурсам. А что при этом известно об их компьютерах? Разумеется, некоторые из них, как правило, тоже являются членами этого же домена, однако в среде Windows членство компьютера в домене, к ресурсам которого он пытается обратиться, не является обязательным требованием. Если при обращении к сетевым ресурсам пользователь указывает корректные параметры учетной записи, он может получать права доступа к любому компьютеру в сети. Имеющийся в системе Windows XP менеджер учетных записей позволяет клиенту, который не является членом домена, еще более упростить процедуру получения доступа к сетевым ресурсам.

Применение концепции изолирования доменов может существенно затруднить «компьютерам-злоумышленникам» процедуру получения доступа к ресурсам домена и разрешить взаимодействие в пределах домена только авторизованным в нем компьютерам. Компьютерам, которые являются членами домена, можно доверять в большей степени, поскольку при всех взаимодействиях между ними используются те механизмы безопасности, которыми администратор домена может централизованно управлять. К таким механизмам относятся групповые политики, шаблоны безопасности, настройка ограничений для программного обеспечения, политики IPsec и Microsoft

Systems Management Server (SMS). Если конфигурация компьютеров находится под контролем, значит, они могут делать только то, что им разрешено. Соответственно, такие компьютеры представляют гораздо меньшую опасность для информационной среды компании, чем неподконтрольные компьютеры злоумышленников, о конфигурации, а зачастую и о существовании которых администратор не имеет ни малейшего представления. Так что уже сама собой напрашивается мысль о необходимости срочного изолирования домена.

Изолирование домена осуществить гораздо проще, чем кажется. Для начала добавим к используемому по умолчанию доменному объекту групповой политики (GPO) следующую политику IPsec.

- Список фильтров: использовать существующий список фильтров «Весь трафик IP» (All IP Traffic).
- Действие фильтра: только Encapsulating Security Payload (ESP), нулевое шифрование (null encryption), проверка целостности SHA-1 (SHA-1 integrity), обязательная защита (require security), запрет взаимодействия между компьютерами без использования протокола IPsec.
- Правило: связать список с действием; для всех сетевых интерфейсов; без туннеля; метод аутентификации — Kerberos, нет отклика по умолчанию.

В данном случае следует использовать ESP-null, поскольку нас интересует только аутентификация каждого пакета, а не шифрование передаваемых данных. Понятие конфиденциальности не ограничивается только аутентификацией и целостностью данных, что обеспечивается хешем SHA-1. Вместо ESP-null можно задействовать заголовок аутентификации IPsec (IPsec Authentication Header (AH)), но при этом данная политика не будет работать с теми системами, которые осуществляют сетевое взаимодействие через устройства, выполняющие функцию трансляции сетевых адресов (NAT).

Теперь нужно создать политику, «открывающую» контроллеры домена, поскольку клиентам необходимо взаимодействовать с ними при аутентификации и получении билета Kerberos, который они будут использовать во всех последующих коммуникациях:

- Список фильтров: фильтры, содержащие адреса или диапазон адресов контроллеров домена.
- Действие фильтра: разрешить.
- Правило: связать список с действием; для всех сетевых интерфейсов; без туннеля; метод аутентификации — любой.

Аналогичные политики потребуются и для тех устройств, которые не могут взаимодействовать через IPsec, таких как сетевые принтеры.

После того как политики будут протестированы и применены, системы, не входящие в состав домена, потеряют возможность взаимодействовать с компьютерами домена, поскольку члены домена требуют использования IPsec для установления соединений с ними, а клиент не сможет получить нужную политику до тех пор, пока не будет включен в соответствующий домен. Если попытаться применить аналогичную политику на компьютере вне домена, это тоже ни к чему не приведет, поскольку для функционирования политики IPsec необходимо использовать аутентификацию через Kerberos, что возможно только в том случае, если компьютер включен в домен. А поскольку данная политика распространяется на все компьютеры домена, они могут взаимодействовать между собой без проблем.

В результате логические рамки сети несколько сужаются, хотя при этом становится затруднительно определить внешнюю границу сети традиционным способом. В данном случае вместо классической сети, напоминающей яйцо с жесткой скорлупой-периметром и мягкой сердцевиной, мы получили структуру, подобную луковице с несколькими вложенными слоями. Таким образом, мы перешли в среду, в которой каждый компьютер каждого слоя будет защищен.

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы
1-2	1-2	1-2	1-4

Оценочные средства: отчет к лабораторной работе (См.: Фонд оценочных средств)

Лабораторная работа № 6
«Организация VPN средствами СЗИ StrongNet»

Форма проведения: **лабораторная работа Цель работы:**

Изучить методы организации VPN средствами СЗИ StrongNet.

Общие сведения.

Система StrongNet предназначена для построения защищенных виртуальных частных сетей, позволяет создать защищенный канал для передачи данных между компьютерами в локальной сети или Интернет. Вся информация передается по этому каналу с использованием туннелирования в зашифрованном виде.

Система StrongNet основана на предварительном распределении ключей. Принцип работы следующий: все данные, передаваемые по защищенному каналу, шифруются с помощью симметричных алгоритмов шифрования. При этом ключи шифрования (сеансовые ключи) передаются между компьютерами при установлении защищенного соединения и шифруются с помощью асимметричного алгоритма шифрования RSA. Открытые и личные ключи, использующиеся при установлении соединения, хранятся в базе данных ключей. Распределение ключей между пользователями осуществляется системным администратором с помощью центра генерации ключей. Таким образом, пользователи сети к моменту установления соединения уже имеют все необходимые ключи.

Кроме защиты данных, передаваемых между двумя компьютерами по сети, StrongNet предоставляет функции персонального межсетевого экрана, который осуществляет фильтрацию входящих и исходящих IP-пакетов по определенным критериям.

Для работы с системой StrongNet необходимо сгенерировать и распределить между пользователями открытые и личные ключи. У каждого пользователя системы StrongNet есть набор ключей, в который входит его личный ключ и открытые ключи других пользователей системы, с которыми он обменивается данными через защищенные каналы. Набор ключей может храниться в файле либо на электронном ключе.

Программа «StrongNet Центр генерации ключей» предназначена для создания базы данных ключей, составления из них наборов, записываемых в файл или на электронный ключ, и распределения этих наборов между пользователями системы. Генерация ключей происходит один раз при создании базы данных.

Постановка задачи

Пусть существует некая организация, в которой в удаленных друг от друга офисах работают два пользователя. Требуется с использованием технологии виртуальных машин создать структуру сети, состоящую из двух виртуальных узлов, и установить защищенное соединение (рис. 5.31). Основная ОС имитирует работу компьютера стороннего наблюдателя и используется для анализа сетевого трафика.

VM 1 **M 2**

StrongNet **StrongNet 2**

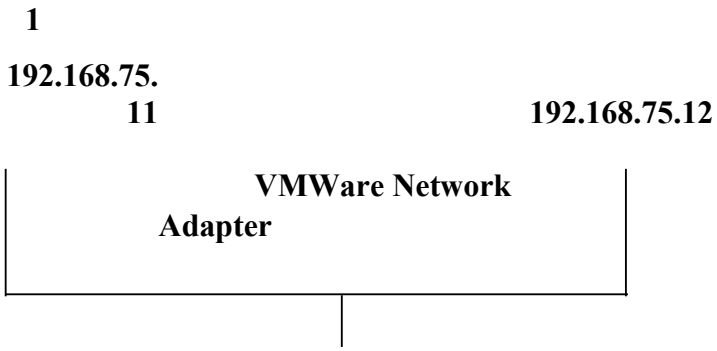


Рис. 1. Схема соединения виртуальных узлов

ВЫПОЛНИТЬ!

1.На рабочем месте открыть два образа ОС Windows 2000. Для каждого образа на вкладке Edit выбрать меню «Virtual Machine Settings» и установить размер потребляемой памяти (Guest size) — 64 MB, а тип сетевого подключения — «VMNet1 (Host Only)». Для обоих образов настроить виртуальные дисководы на единый файл. Запустить виртуальные ОС.

2.Настроить IP-адреса виртуальных машин (например, для первой ОС —

192.168.75.11, для второй ОС — 192.168.75.12). С помощью программ ipconfig и ping убедиться в правильной настройке сетевых адресов.

132

3.Осуществить захват трафика в основной ОС, убедиться в возможности анализа передаваемых ICMP-пакетов.

4.Установить систему StrongNet в обе виртуальные ОС, следуя указаниям установочной программы.

Генерация и распространение ключевой информации

Для успешной работы системы StrongNet необходимо создать базу данных ключей. Дистрибутив ключей для каждого сетевого узла размещен в файле с расширением «DST». Исходные ключи зашифрованы на парольной фразе и потому недоступны третьим лицам непосредственно из DST-файла. Чтобы создать базу данных ключей нужно запустить программу «Центр генерации ключей».

ВЫПОЛНИТЬ!

5.На одной из систем запустить программу «StrongNet Центр генерации ключей». В меню «Действие» выбрать пункт «Создать БД ключей». В появившемся окне установить количество генерируемых ключей — 2. Сохранить базу данных ключей.

6.Сгенерировать ключи для двух пользователей с учетом их дальнейшего взаимодействия. Для этого в правой части главного окна дважды щелкнуть левой кнопкой мыши на элементе «Пользователь 1». В появившемся окне «Создание КК» ввести имя, в списке «Все» выбрать Пользователь 2 и нажать кнопку « >> ». Нажать кнопку «Далее». В появившемся диалоговом окне «Запись КК» выбрать тип внешнего ключа — «Файл». Указать путь и имя файла, в котором будет храниться созданный набор ключей для Пользователя 1 и открытый ключ Пользователя 2. Аналогичные действия произвести для Пользователя 2.

7.После завершения работы мастера скопировать набор ключей Пользователя 2 на дискету (виртуальную дискету).

Настройка СЗИ StrongNet

ВЫПОЛНИТЬ!

8.В одной из виртуальных систем открыть главное окно программы StrongNet и нажать кнопку «Развернуть» (рис. 5.32).

9.На вкладке «Ключи» (рис. 5.33) выбрать тип внешнего ключа – файл. Указать файл с набором ключей Пользователя 2 и нажать кнопку «Загрузить». Переключатель «Загружать ключи при старте» поставить в состояние

«Включено».

10.Во второй ОС аналогично загрузить набор ключей Пользователя 2, сохраненный на дискете.

Рис. 2. Главное окно программы «StrongNet»

11.Используя вкладку «Настройки» (рис. 5.34) сделать так, чтобы сеансовый ключ в процессе работы защищенного соединения периодически менялся. Он может меняться по истечении некоторого промежутка времени, для этого переключатель «Генерировать ключ каждые» устанавливается во включенное состояние и в поле «Секунды» указывается длина соответствующего временного интервала. Чтобы защищенное соединение периодически проверялось на предмет активности, переключатель «Подтверждать соединение» устанавливается во включенное состояние и в поле «Секунды» указывается длина периода в секундах. Для вступления в силу сделанных изменений нажать кнопку «Применить».

Рис. 3. Загрузка ключевой информации Рис. 4. Настройка параметров обновления ключевой информации

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы
1-2	1-2	1-2	1-4

Оценочные средства: отчет к лабораторной работе (См.: Фонд оценочных средств)

Лабораторная работа № 7
«Принципы защиты программно-аппаратным комплексом SecretNet»

Форма проведения: **лабораторная работа Цель работы:**

Изучить принципы защиты программно-аппаратным комплексом SecretNet.

Общие сведения.

Система *Secret Net* предназначена для организации защиты информации в локальных вычислительных сетях, построенных на основе операционных систем *Windows NT*, *Windows 2000*, *Windows'9x* и *MP-RAS*. Она позволяет организовать эффективную защиту информации, циркулирующей в автоматизированной информационной системе предприятия.

Система *Secret Net* не подменяет собой защитные механизмы операционных систем, а дополняет их в части защиты рабочих станций и серверов сети, позволяя тем самым повысить защищенность всей автоматизированной информационной системы в целом.

Система защиты *Secret* позволяет:

- решать различные задачи по обеспечению информационной безопасности (сбор оперативных данных, контроль доступа в помещения и т.д.) в рамках единой системы управления безопасностью организации;
- реально объединить в единую систему различные средства обеспечения безопасности - средства криптографической защиты, средства анализа защищенности и оповещения о сетевых атаках, средства защиты от НСД;
- оперативно получать актуальную информацию о реальном состоянии защищенности информационной системы и оценивать ее соответствие требованиям, существующим в организации;
- значительно упростить управление доступом сотрудников организации к ресурсам информационной системы за счет унификации номенклатуры управляемых объектов и прав доступа.

Дополнительно к стандартным механизмам защиты, реализованным в ОС *Windows'9x*, *Windows NT*, *Windows 2000* и *MP-RAS* система *Secret Net* обеспечивает:

- Опознавание (идентификацию) пользователей при помощи специальных аппаратных средств (*Touch Memory*, *eToken*, *Smart Card*). Возможна организация криптографической аутентификации пользователя сервером безопасности.
- Избирательное (дискреционное) управление доступом средствами *Secret Net 9x*. Дополнительно к средствам избирательного управления доступом ОС *Windows*

NT и *Windows 2000* системы *Secret Net NT* и *Secret Net 2000* обеспечивают избирательное управление доступом к локальным логическим дискам и портам.

- Полномочное (мандатное) разграничение доступа к файлам (на локальных и сетевых дисках) в соответствии со степенью конфиденциальности содержащихся в них сведений и уровнем допуска пользователя.

- Возможность подключения и использования средств криптографической защиты данных, передаваемых по сети, и данных, хранимых в файлах на внешних носителях (жесткие и гибкие магнитные диски и т.д.). Обмен данными между всеми или отдельными рабочими станциями сети может осуществляться в криптографически защищенном виде.

- Централизованное оперативное управление доступом пользователей к совместно используемым ресурсам, как в одноранговой, так и в доменной сети.

- Оперативный контроль работы пользователей сети. Оповещение администратора безопасности о событиях несанкционированного доступа. Централизованный сбор и анализ содержимого журналов регистрации.

- Контроль целостности программ, используемых ОС и пользователем.

Возможны следующие варианты применения системы *Secret Net*:

-для защиты информации, хранимой и обрабатываемой на **автономном компьютере**, работающем под управлением ОС семейства *Windows'9x* (*Windows 95*, *OSR2*, *Windows 98*);

- для защиты локальных ресурсов **рабочей станции локальной вычислительной сети**, работающей под управлением ОС семейства *Windows'9x* (*Windows 95*, *OSR2*, *Windows 98*);

- как комплексное средство защиты локальных ресурсов компьютера или рабочей станции сети, работающей под управлением ОС семейства *Windows'9x* (*Windows 95*, *OSR2*, *Windows 98*), используемое совместно с *Электронным замком "Соболь"*.

Система защиты информации *Secret Net* обеспечивает совместную работу с сертифицированными средствами криптографической защиты информации.

Схема размещения и взаимодействия компонент и подсистем, входящих в состав серверной части системы *Secret Net* представлена на Рис.2. Эта часть системы размещается (устанавливается) на выделенном компьютере и взаимодействует с клиентской частью системы защиты.

Использование механизма активных объектов позволяет с минимальными затратами осуществлять расширение функциональных возможностей сервера безопасности. К числу активных можно отнести следующие объекты:

"**Администратор**" - обеспечивает взаимодействие с программами подсистемы управления. При создании этого объекта ему присваиваются специальные привилегии пользователя, от имени которого осуществляется управление; "**Клиент**" - используется для взаимодействия с агентами клиентов сервера безопасности. Эти объекты хранят всю оперативную информацию о состоянии механизмов защиты клиентов; "**Установщик**" - обеспечивает взаимодействие с программами установки при установке клиентов на рабочие станции или серверы сети.

Ядро сервера безопасности осуществляет аутентификацию клиентов и программ подсистемы управления. В текущей версии системы аутентификация проводится с использованием секретных личных ключей сотрудников. В результате

аутентификации для каждого соединения генерируется сеансовый ключ. Дальнейший обмен данными между сервером безопасности и взаимодействующими с ним прикладными программами осуществляется в защищенном виде.

Универсальный интерфейс с СУБД. Активные объекты сервера безопасности могут получать доступ к сведениям, хранящимся в ЦБД системы защиты. Для организации доступа к данным, хранящимся в ЦБД, используется специальный, СУБД независимый интерфейс. Этот интерфейс позволяет использовать различные типы СУБД для организации и ведения ЦБД системы защиты.

Система управления базами данных (СУБД) обеспечивает управление данными, хранящимися в ЦБД системы защиты. В текущей версии сервера безопасности используется СУБД *Oracle 8.0*.

Планировщик задач обеспечивает периодический запуск различных внешних подсистем сервера, имеющих непосредственный доступ к ЦБД системы защиты.

Криптографическая подсистема. Основу этой подсистемы составляет так называемое криптографическое ядро, включающее менеджер алгоритмов и модули, реализующие различные криптографические алгоритмы. Менеджер алгоритмов реализует универсальный криптографический интерфейс, обеспечивающий независимое от типа криптографического алгоритма взаимодействие прикладных программ с этой подсистемой, а также возможность добавления новых алгоритмов.

Коммуникационная подсистема обеспечивает защищенный обмен данными по протоколам *TCP/IP* и *IPX* между сервером безопасности и другими компонентами системы *Secret Net*, например, с клиентами на рабочих станциях и серверах сети. Весь обмен данными производится в защищенном виде. Передаваемые данные подвергаются сначала имитозащите, потом сжатию, а затем криптографической защите.

Таким образом, сервер безопасности обеспечивает:

- аутентификацию клиентов и установление с ними защищенных соединений;
- взаимодействие с программами управления и ведение ЦБД системы защиты;
- синхронизацию содержимого ЦБД и ЛБД системы защиты;
- прием от клиентов и предварительную обработку журналов регистрации;
- сбор, хранение и выдачу сведений об активности клиентов;
- прием и сохранение сообщений о событиях НСД;
- получение управляющих воздействий от программ подсистемы управления и оперативную передачу этих воздействий клиентам;
- управление криптографическими параметрами системы защиты;
- планирование и применение различных внешних подсистем.

Подсистема управления

Подсистема управления обеспечивает:

- отображение состояния защищаемых рабочих станций и серверов сети;
- оперативное управление защитой рабочих станций и серверов сети;
- ведение ЦБД системы защиты (управление пользователями, настройками компьютеров и т.д.);
- получение справок и отчетов из ЦБД системы защиты.

Компонента управления ЦБД системы защиты обеспечивает ведение ЦБД на сервере безопасности, корректировку хранимых в ЦБД сведений о различных объектах, просмотр содержимого системных журналов и генерацию различных отчетов.

Для упрощения распределения полномочий пользователей и настройки режимов

работы компьютеров используется специальный ***механизм шаблонов***. Шаблон представляет собой некоторую совокупность значений параметров, которой присвоено символическое имя. Применение шаблона к объекту управления приводит к присвоению ему значений, содержащихся в шаблоне. Использование шаблонов позволяет администратору безопасности типизировать наборы параметров для пользователей и наборы настроек компьютеров, применяемых в защищаемой информационной системе.

В качестве ***объектов управления*** выступают объекты предметной области. Это дает возможность использовать при управлении формализованные электронные документы (заявки) и контролировать состояние информационной безопасности корпоративной сети на основе типовых отчетных документов. События, происходящие в информационной системе, регистрируются в ряде журналов, перечень которых приведен в Табл.1.

Название журнала	Содержание
Журнал конфликтов обратной синхронизации	Содержит записи, необходимые для разрешения конфликтов, возникающих при обратной синхронизации
Журнал событий	Содержит записи обо всех событиях, произошедших на защищаемых рабочих станциях и серверах
Журнал событий НСД	Содержит записи о событиях НСД, произошедших на защищаемых рабочих станциях и серверах
Системный журнал	Содержит записи, регистрирующие внутренние события сервера безопасности
Журнал аудита	Содержит регистрационные записи об управляющих действиях администраторов разных уровней

Средства генерации отчетов позволяют получать различные типы отчетов, в которых данные представлены под интересующим углом зрения.

Компонента оперативного управления предназначена для получения оперативной информации о состоянии рабочих станций и серверов сети, их текущих настройках, списках работающих (активных) пользователей, происшедших событиях НСД и т.д. Для защиты данных, передаваемых между компонентами системы управления и сервером безопасности, используется ***криптографическая подсистема*** клиентской части рабочей станции, на которой установлена подсистема управления. Все управляющие воздействия администратора передаются серверу безопасности в виде команд. Сервер безопасности получает, обрабатывает эти команды и управляет выполнением соответствующих действий. В свою очередь сервер безопасности передает подсистеме управления информацию о состоянии всех рабочих станций.

Состав клиентской части

Клиентская часть системы *Secret Net* состоит из следующих компонент и подсистем:

- агент сервера безопасности (*AGENT*);
- локальная база данных (ЛБД) системы защиты;
- подсистема идентификации;
- подсистема избирательного управления доступом;
- подсистема полномочного управления доступом;
- подсистема контроля целостности;
- подсистема криптографической защиты;
- компонента защиты от загрузки;

На Рис. представлена схема размещения и взаимодействия компонент и подсистем, входящих в состав клиентской части системы *Secret Net*. Эта часть системы защиты может размещаться (устанавливаться) на любой рабочей станции или сервере автоматизированной информационной системы предприятия.

Агент сервера безопасности

Агент сервера безопасности (*AGENT*) представляет собой программу, которая запускается на защищенной рабочей станции при ее включении и загрузке. Эта программа взаимодействует с другими компонентами и подсистемами клиентской части системы *Secret Net* и осуществляет взаимодействие с сервером безопасности.

В процессе работы системы защиты агент сервера безопасности:

- устанавливает соединение с сервером безопасности и восстанавливает соединение после перезапуска рабочей станции или сервера безопасности;
- синхронизирует системное время рабочей станции с системным временем сервера безопасности;
-выполняет опознавание (аутентификацию) пользователя на сервере безопасности при входе пользователя в систему;
-обеспечивает обмен данными и обработку команд, поступающих от сервера безопасности;
- периодически оповещает сервер безопасности о состоянии рабочей станции;
- обрабатывает оперативные сообщения о попытках выполнения пользователем несанкционированных действий (НСД), поступающие от подсистем клиентской части системы защиты, и оперативно передает эти сообщения серверу безопасности;
-осуществляет ведение локальной базы данных (ЛБД) системы защиты.

Локальная база данных системы защиты

Локальная база данных (ЛБД) предназначена для хранения сведений, необходимых для работы защищенной рабочей станции. ЛБД используется агентом сервера безопасности и подсистемой идентификации пользователя. В ЛБД хранится информация следующих основных категорий:

- о пользователях рабочей станции (имя, полномочия пользователей, права доступа к конфиденциальной информации и т.д.);
- о локальных ресурсах рабочей станции, переданных в совместное использование и полномочиях пользователей по доступу к этим ресурсам;
- о настройках системы защиты для данной рабочей станции.

Агент по команде сервера безопасности обновляет информацию , хранящуюся в ЛБД, в соответствии с информацией ЦБД. Подсистема идентификации пользователя извлекает из ЛБД сведения, необходимые для его идентификации и аутентификации.

Подсистема идентификации

Подсистема идентификации включает в себя модуль идентификации пользователя, а также, если они установлены на рабочей станции, средства аппаратной поддержки (например, *Secret Net TM Card*, *Электронный замок "Соболь"* и т.д.) и программу-драйвер, с помощью которой осуществляется управление этими аппаратными средствами. На Рис.4 представлена схема размещения и взаимодействия модулей и компонент, входящих в состав подсистемы идентификации.

Подсистема контроля целостности

Подсистема контроля целостности предназначена для контроля за неизменностью параметров объектов с целью защиты их от модификации. Для этого в соответствии с расписанием контроля определяются текущие параметры проверяемых объектов и сравниваются с ранее полученными эталонными значениями контролируемых параметров. Подсистема включает в себя следующие компоненты:

Подсистема полномочного управления доступом

Подсистема полномочного управления доступом обеспечивает разграничение доступа пользователей к конфиденциальной информации, хранящейся в файлах на локальных и сетевых дисках. Доступ осуществляется в соответствии с категорией конфиденциальности, присвоенной информации, и уровнем допуска пользователя к конфиденциальной информации.

Подсистема криптографической защиты информации

Криптографическая защита используется для шифрования информации, хранящейся в файлах на сетевых и локальных дисках, и шифрования сетевого трафика с целью повышения защищенности конфиденциальной информации.

Архитектура подсистемы криптографической защиты обеспечивает:

- Независимость прикладных программ от схем генерации и распределения ключей шифрования и электронной цифровой подписи, а также независимость от реализаций криптографических алгоритмов (программных или аппаратных);
- Возможность использования одних и тех же ключей различными прикладными программами (процессами) без передачи секретных значений;
- Использование одних и тех же алгоритмов, как прикладными программами, так и модулями систем защиты, работающими на уровне ядра операционной системы.

Компонента защиты от загрузки

Компонента защиты от загрузки предназначена для защиты рабочей станции от загрузки ОС со съемных носителей (гибких дисков или CD ROM дисков). Компонента защиты от загрузки представляет собой ПЗУ, программное обеспечение которого позволяет при инициализации компьютера (сразу после загрузки BIOS) осуществить запрет на загрузку операционной системы со съемных носителей. ПЗУ компоненты защиты от загрузки устанавливается на плату аппаратной поддержкисистемы *Secret Net*.

Система защиты *Secret Net* дополняет операционные системы *Windows NT*, *Windows 2000, Windows'9x* и *MP-RAS* рядом защитных функций, которые можноотнести к следующим группам средств защиты:

1. Средства защиты от несанкционированного входа в систему:

- механизм идентификации и аутентификации пользователей, обеспечивающий (в том числе с помощью аппаратных средств) защиту от входа постороннего пользователя в систему при загрузке компьютера;
- функция временной блокировки компьютера, обеспечивающая защиту работающего компьютера от постороннего пользователя;
-функция программной защиты от загрузки с гибкого диска, обеспечивающая защиту локальных жестких дисков в случае загрузки компьютера с гибкого диска;
- аппаратные средства внешней защиты, предотвращающие загрузку операционной системы с гибкого диска и блокирующие вход в систему, минуя внешнюю защиту.

2. Средства управления доступом к ресурсам:

- разграничение доступа пользователей к ресурсам компьютера с использованием **механизмов избирательного и полномочного управления доступом**;

- создание для любого пользователя ограниченной **замкнутой среды по** (списка разрешенных для запуска программ).

3. Средства криптографической защиты данных:

- шифрование информации, хранящейся в файлах на сетевых и локальных дисках;

- вычисление и проверка электронной цифровой подписи (ЭЦП).

4. Средства регистрации и оперативного контроля:

- ведение журнала регистрации событий, имеющих отношение к безопасности системы. Работа с журналами, управление временем хранения и с удалением записей;

- контроль целостности различных объектов.

Пользователь, имеющий привилегии администратора безопасности, может активизировать на компьютере различные комбинации защитных механизмов системы, выбирая из них только необходимые и устанавливая соответствующие режимы их работы.

Аппаратные средства внешней защиты. В системе *Secret Net* предусмотрена аппаратная поддержка описанных выше механизмов внешней защиты. Она обеспечивается специальными техническими устройствами - например, платами *Secret Net TM Card* или *Secret Net Card*. Аппаратные средства внешней защиты обеспечивают:

- защиту от загрузки операционной системы с гибкого диска и проникновения в систему, минуя внешнюю защиту;

- идентификацию пользователя с помощью аппаратных средств идентификации (чтение информации из персонального идентификатора пользователя).

Электронные замки "Соболь-PCI" и "Соболь"

Изделия "Программно-аппаратный комплекс "Соболь-PCI" и "Электронный замок "Соболь" версии 1.0" предназначены для организации защиты компьютера от НСД посторонних пользователей. Они обеспечивает:

- идентификацию и аутентификацию пользователей с помощью УВИП на базеTouch Memory;

- блокировку загрузки операционной системы с внешних съёмных носителей;

- блокировку пользователя при превышении им количества допустимых попыток ввода неправильного пароля;

- контроль целостности программной среды компьютера до загрузки ОС;

- регистрацию событий, связанных с попытками входа пользователей и результатами работы подсистемы контроля целостности.

Изделия Secret Net Touch Memory Card PCI и Secret Net Touch Memory Card

Изделия Secret Net Touch Memory Card PCI и Secret Net Touch Memory Card предназначена для идентификации и аутентификации пользователей; блокировки загрузки операционной системы с внешних съёмных носителей.

Сетевой адаптер с микросхемой Secret Net ROM BIOS Сетевой адаптер в качестве изделия аппаратной поддержки системы Secret Net предназначен для запрета загрузки ОС со сменных носителей (для Secret Net 9x/NT/2000), а также идентификации и аутентификации пользователей без электронного идентификатора (для Secret Net 9x).

Изделие Secret Net Card Изделие Secret Net Card предназначено для запрета загрузки операционной системы с внешних съёмных носителей (для Secret Net 9x/NT/2000), а также идентификации и аутентификации пользователей без электронного идентификатора (для Secret Net 9x).

В системе *Secret Net* существуют средства, позволяющие ограничить доступ пользователей к исполняемым файлам без использования системы атрибутов. Для этой цели применяется ***механизм замкнутой программной среды***, позволяющий сформировать для любого пользователя компьютера программную среду, определив

перечень программ, разрешенных ему для запуска. Этот механизм ограничивает возможности пользователя по запуску программ только теми программами, которые действительно необходимы ему для выполнения своих служебных обязанностей. Таким образом, пользователь не сможет запустить программы, не входящие в список разрешенных для запуска программ, в том числе и с гибких дисков (если они ему доступны). Кроме того, пользователь не сможет запустить программы, входящие в список разрешенных для запуска программ, если у файлов программ отсутствует владелец, а также программы, не доступные пользователю на изменение (переименование).

Запуск программ пользователями контролирует ***диспетчер доступа*** системы *Secret Net*. Когда пользователь (программа, запущенная пользователем) осуществляет попытку запуска какой-либо программы, диспетчер доступа проверяет, включена ли эта программа в список программ, разрешенных для запуска данному пользователю. Если программа содержится в списке, диспетчер доступа разрешает ее запуск. Если пользователю не разрешается запускать данную программу - информация о ней отсутствует в списке разрешенных для запуска программ, у файла программы отсутствует владелец и т.д., диспетчер доступа блокирует запуск программы. В этом случае в системном журнале регистрируется попытка НСД.

Списки разрешенных для запуска программ представляют собой обычные текстовые файлы, содержащие в каждой строке полный путь к файлу программы, запуск которой разрешен.

В системе *Secret Net* предусмотрено несколько режимов идентификации и аутентификации с использованием аппаратных средств. Это дает возможность проводить внедрение аппаратных средств поэтапно. Основными режимами являются "Мягкий" и "Жесткий". В первом случае любой пользователь может войти в систему двумя способами: 1) предъявив персональный идентификатор, 2) указав свое имя, во втором - вход в систему любого пользователя разрешен только при предъявлении персонального идентификатора.

Средства разграничения доступа.

Механизм избирательного управления доступом. Механизм избирательного управления доступом обеспечивает разграничение доступа пользователей к локальным ресурсам компьютера, используя следующие средства системы *Secret Net*:

- систему атрибутов *Secret Net* и средства управления атрибутами;
- средства управления доступом к аппаратным ресурсам компьютера;
- средства управления доступом к ресурсам операционной системы;
- диспетчер доступа

Каждый зарегистрированный пользователь компьютера наделяется определенными правами доступа к ресурсам этого компьютера

Система атрибутов Secret Net. Система защиты *Secret Net* использует свою систему атрибутов для организации избирательного доступа пользователей к ресурсам файловой системы. Эти атрибуты не подменяют собой атрибуты ОС *Windows'9x* и *MS DOS*, присваиваемые файлам и каталогам. Атрибуты *Secret Net* прозрачны (незаметны) для этих операционных систем и могут присваиваться как файлам и каталогам, так и логическим дискам.

Атрибуты *Secret Net* подразделяются на три группы:

- атрибуты владения ресурсом;
- атрибуты управления доступом к ресурсу;
- дополнительные атрибуты.

Атрибуты владения ресурсом определяют пользователя, являющегося владельцем ресурса, и группу пользователей - владельцев ресурса. Присвоенные ресурсу атрибуты владения содержат сведения о владельце и группе владельцев ресурса.

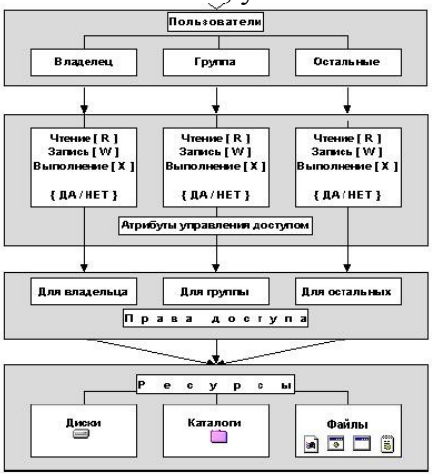
Атрибуты владения разделяют всех пользователей *Secret Net* по отношению к данному ресурсу на три категории: владелец ресурса (“**Владелец**”); группа владельцев ресурса (“**Группа**”); остальные пользователи компьютера (“**Остальные**”).

Для каждой из этих категорий пользователей назначаются свои ***атрибуты управления доступом***, определяющие права доступа пользователей к ресурсу. Таким образом, каждый пользователь компьютера наделяется определенными правами доступа к данному ресурсу в зависимости от того, к какой из трех указанных категорий он принадлежит. В системе *Secret Net* действуют следующие общие правила владения ресурсами. 1) Ресурс, для которого не определены атрибуты владения, считается “**общим**”. Любой зарегистрированный пользователь компьютера может производить с “**общим**” ресурсом любые действия, кроме присваивания ему своих атрибутов владения и управления доступом (право на выполнение этого действия определяется привилегиями на администрирование системы защиты). Пользователь, первым установивший свои атрибуты владения на “**общий**” ресурс, становится его владельцем. 2) При создании нового ресурса (каталога или файла), ему автоматически

присваиваются определенные атрибуты владения и доступа. Значения устанавливаемых атрибутов соответствуют значениям атрибутов по умолчанию, которые определены в паспорте пользователя, создавшего ресурс. 3) Возможность изменения атрибутов владения, присвоенных существующим ресурсам, ограничена и определяется привилегиями на администрирование системы защиты, предоставленными данному пользователю.

Атрибуты управления доступом к ресурсу

Атрибуты управления доступом определяют права доступа к ресурсу различных категорий пользователей (“**Владелец**”, “**Группа**”, “**Остальные**”). Принадлежность текущего пользователя компьютера к одной из этих категорий определяется ***атрибутами владения***, установленными на данный ресурс.



В системе *Secret Net* действуют следующие общие правила управления доступом к ресурсам.

1) Система не отображает имя ресурса, если у текущего пользователя отсутствует доступ к этому ресурсу. Это правило не распространяется на пользователей, обладающих соответствующими привилегиями на работу с системой.

2) Если права доступа пользователя к ресурсу не позволяют ему выполнить некоторую операцию с ресурсом, система *Secret Net* блокирует выполнение этой операции. Это правило не действует, если установлен “**мягкий режим**” работы с атрибутами, или в том случае, когда пользователю предоставлены соответствующие привилегии на работу с системой

3) При создании нового ресурса (каталога или файла), ему автоматически присваиваются определенные атрибуты владения и доступа. Значения устанавливаемых

атрибутов соответствуют значениям атрибутов по умолчанию, которые определены в паспорте пользователя, создавшего ресурс.

4) Возможность изменения атрибутов доступа, присвоенных существующим ресурсам, ограничена и определяется привилегиями на администрирование системы защиты, предоставленными данному пользователю.

Дополнительные атрибуты

Кроме атрибутов владения и управления доступом в системе *Secret Net* используются ***дополнительные атрибуты***, расширяющие возможности организации работы с файлами. Эти атрибуты устанавливаются только на файлы. Всего существует четыре дополнительных атрибута: “**Полный доступ**” - имеет смысл только для программ. Устанавливает для программы специальный режим работы. В этом режиме не контролируется доступ программы к ресурсам файловой системы (дискам, каталогам и файлам), аппаратным ресурсам (коммуникационным портам и принтерам) и ресурсам операционной системы (системным файлам, ключам реестра и т.д.). Попытки доступа программы к этим ресурсам не регистрируются в системном журнале. При включенном режиме полномочного управления

доступом все попытки доступа программы к конфиденциальным ресурсам **контролируются**;

“**Аудит чтения**” - устанавливает для файла режим регистрации в системном журнале всех попыток чтения информации из файла;

“**Аудит записи**” - устанавливает для файла режим регистрации в системном журнале всех попыток осуществить запись информации в файл;

“**Только чтение**” - включает для файла режим, при котором реальный доступ к этому файлу разрешен только на чтение, но программе, которая осуществляет доступ к файлу на запись, возвращается признак успешного завершения операции изменения файла. Этот атрибут используется для обеспечения совместимости системы защиты с некоторыми специализированными программами.

Управление атрибутами Secret Net. Средства управления атрибутами *Secret Net* обеспечивают:

присвоение атрибутов ресурсам файловой системы;

проверку прав доступа пользователей к ресурсам в соответствии с присвоенными ресурсам атрибутами.

Атрибуты доступа и владения могут быть присвоены ресурсам файловой системы несколькими способами:

1) Автоматически системой *Secret Net* при ее установке на компьютер;

2) Автоматически системой *Secret Net* при создании файла или каталога;

3) “Вручную” пользователем при помощи компонент *Secret Net*

Наследование атрибутов доступа. В системе *Secret Net* приняты следующие правила наследования атрибутов доступа.

1) Атрибуты управления доступом к диску распространяются на все каталоги, подкаталоги и файлы, находящиеся на данном диске.

2) Атрибуты управления доступом к каталогу распространяются на все файлы и подкаталоги, а также на все файлы подкаталогов, входящие в состав данного каталога.

3) В части ограничения прав доступа приоритет атрибутов доступа к диску выше, чем приоритет атрибутов доступа к каталогам и файлам данного диска, а приоритет атрибутов доступа к каталогу выше приоритета атрибутов доступа к его файлам и подкаталогам.

4) В части расширения прав доступа приоритет атрибутов доступа к диску или каталогу считается ниже, чем приоритет атрибутов подкаталогов и файлов этого диска или каталога

5) Привилегии на работу с системой имеют наивысший приоритет при определении эффективных прав доступа пользователя к ресурсу и отменяют соответствующие ограничения доступа, заданные атрибутами доступа к ресурсу.

Управление доступом к аппаратным ресурсам. Средства управления доступом к аппаратным ресурсам обеспечивают ограничение прав доступа зарегистрированных пользователей к следующим аппаратным ресурсам компьютера:

- локальным принтерам; - сетевым принтерам; - коммуникационным портам (COM, LPT, PS2); - дисководам, приводам CD ROM.

Для любого пользователя компьютера может быть установлен запрет доступа к любому из указанных аппаратных ресурсов. В том случае, если доступ текущего пользователя к ресурсу запрещен, все обращения средствами операционной системы к этому ресурсу блокируются.

Управление доступом к ресурсам операционной системы. Средства управления доступом к ресурсам операционной системы обеспечивают ограничение прав доступа зарегистрированных пользователей к следующим ресурсам операционной системы:

- системным файлам CONFIG.SYS и AUTOEXEC.BAT;
- ключам системного реестра ОС *Windows*;
- системному времени;
- диалогам настройки параметров работы ОС *Windows*.

Для любого зарегистрированного пользователя компьютера может быть установлен запрет доступа к любому из указанных ресурсов операционной системы. Если доступ текущего пользователя к ресурсу запрещен, любые обращения к этому ресурсу будут блокироваться.

Система *Secret Net* включает в свой состав средства, позволяющие организовать полномочное управление доступом пользователей к ресурсам файловой системы компьютера. Полномочное управление доступом осуществляется только по отношению к логическим дискам и каталогам и распространяется на все файлы и подкаталоги, находящиеся на дисках или содержащиеся в каталогах. При организации полномочного управления доступом для каждого пользователя компьютера устанавливается некоторый уровень допуска к конфиденциальной информации, определяющий его права на доступ к конфиденциальным данным. Всем локальным дискам, подключенным сетевым дискам и каталогам, находящимся на этих дисках, назначается категория конфиденциальности, которая определяется включением диска или каталога в специальные списки, хранящиеся в файлах SLIST.DAT и SSLIST.DAT в каталоге C:\-SNET-\. Категории конфиденциальности соответствует уровень доступа к конфиденциальной информации, устанавливаемый для пользователей компьютера.

В системе *Secret Net* используются следующие три категории конфиденциальности информации (в порядке возрастания уровня конфиденциальности: “**Нет**” (информация доступна пользователю с любым уровнем допуска); “**Конфиденциально**”; “**Строго конфиденциально**”. Разграничение доступа к конфиденциальным ресурсам осуществляется следующим образом. Когда пользователь осуществляет попытку доступа к конфиденциальному ресурсу, ***диспетчер доступа*** *Secret Net* определяет категорию конфиденциальности данного ресурса, считывая информацию, содержащуюся в файлах SLIST.DAT и SSLIST.DAT. Затем категория конфиденциальности ресурса сопоставляется с уровнем допуска к конфиденциальной информации текущего пользователя. Если текущий пользователь не превышает свой уровень допуска, осуществляя доступ к конфиденциальному ресурсу, система защиты санкционирует доступ к ресурсу. Иначе система защиты блокирует доступ к ресурсу.

Механизм контроля целостности. используется в системе *Secret Net* для повышения надежности ее работы. Он осуществляет контроль целостности следующих объектов: системных программ - ядра и исполняемых файлов системы; разрешенных для запуска программ - исполняемых файлов, составляющих список разрешенных для запуска

программ, если для пользователя установлена замкнутая программная среда и включен режим контроля целостности программ; каталогов, файлов, элементов системного реестра, список которых определен пользователем, наделенным соответствующими привилегиями на администрирование системы защиты. Для всех проверяемых объектов составляются ***пакеты контроля целостности***. Эти пакеты содержат контрольные суммы всех проверяемых файлов и полный путь к каждому из них. Контрольные суммы рассчитываются с использованием хеш-функций или по оригинальному алгоритму собственной разработки.

Контроль целостности системных программ и разрешенных для запуска программ осуществляется при загрузке компьютера. Проверка файлов из списка, составленного администратором, осуществляется как при загрузке компьютера, так и согласно расписанию проверки, определенному администратором. Процедура контроля целостности осуществляется следующим образом. Вычисляются контрольные суммы всех проверяемых файлов, список которых содержится в пакете контроля целостности. Осуществляет сравнение полученных контрольных сумм с ранее вычисленными контрольными суммами этих же файлов, содержащимися в пакете контроля целостности. Если хотя бы для одного из проверяемых объектов вычисленная контрольная сумма не сошлась с контрольной суммой хранящейся в пакете контроля целостности, результат проверки считается отрицательным, а целостность контролируемых объектов - нарушенной. Реакция системы *Secret Net* на нарушение целостности определяется настройкой системы защиты. Эта настройка индивидуальна для каждого пользователя компьютера.

Все объекты системы *Secret Net* подразделяются на два основных типа:

объекты, с помощью которых осуществляется управление средствами защиты компьютера, или объекты управления;

объекты, защищаемые средствами системы *Secret Net* , или защищаемыеобъекты.

Объектами управления в системе *Secret Net* являются пользователи и группы пользователей.

Защищаемыми объектами в системе *Secret Net* являются ресурсы компьютера.

Пользователи. В системе *Secret Net* каждому реальному пользователю компьютера ставится в соответствие объект системы защиты - “**Пользователь**”. Свойства этого объекта

определяют статус реального пользователя компьютера в системе защиты и его права на доступ к ресурсам компьютера.

Привилегии пользователя

Статус пользователя в системе *Secret Net* определяется предоставленными этому пользователю привилегиями. Привилегии пользователя делятся на две группы:

привилегии на работу с системой , разрешающие пользователю превышать вои права на доступ к ресурсам компьютера и игнорировать некоторые другие ограничения его работы;

привилегии на администрирование системы защиты, позволяющие пользователю управлять работой системы защиты, т.е. выполнять функции администрирования.

Привилегии пользователя на работу с системой расширяют права доступа пользователя к ресурсам файловой системы: локальным дискам, каталогам, файлам, а также к

аппаратным ресурсам и ресурсам операционной системы.

Предоставив пользователю любую из привилегий **“Видимость…”**, администратор тем самым разрешает во всех программах, отображающих ресурсы файловой системы, показывать пользователю имена логических дисков, каталогов или файлов, доступ к которым ему запрещен. Привилегии **“Без атрибутов на…”** отменяют для пользователя действие атрибутов доступа и владения, установленных на локальных дисках, каталогах или файлах. При этом пользователь наделяется правами полного доступа к этим ресурсам.

Привилегия **“Без ограничений по настройкам”** разрешает игнорировать определенные ограничения при работе пользователя с ресурсами файловой системы, аппаратными ресурсами и ресурсами операционной системы.

Привилегии пользователя на администрирование системы защиты определяют статус пользователя. В зависимости от предоставленных привилегий на администрирование, каждый пользователь может быть отнесен к одной из трех категорий:

- администратор безопасности - пользователь, наделенный всеми привилегиями на администрирование системы защиты;
- привилегированный пользователь - пользователь, наделенный некоторыми привилегиями на администрирование системы защиты;
- рядовой пользователь - пользователь, не имеющий привилегий на администрирование системы защиты.

Наделяя пользователя соответствующими привилегиями на администрирование, администратор безопасности может разрешить ему выполнять следующие действия по управлению работой системы защиты:

- управлять работой пользователей и групп пользователей (создавать, удалять и переименовывать пользователей и группы пользователей; управлять составом групп; изменять свойства пользователей);
- управлять атрибутами системы защиты (изменять атрибуты своих, общих и чужих ресурсов);
- управлять параметрами настройки системы защиты;
- просматривать, удалять и выводить на печать записи системного журнала;
- переустанавливать, удалять и отключать систему защиты.

Установить систему SecretNet на испытуемый компьютер
2. Настроить систему SecretNet для работы 2х пользователей (суперпользователь и пользователь)
3. Настроить систему журналирования
4. Настроить «Замкнутую среду» работы
5. Включить «Жесткий режим» работы системы
6. Настроить систему контроля целостности
7. Настроить систему маркировки при выводе на печать

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы
1-2	1-2	1-2	1-4

Оценочные средства: отчет к лабораторной работе (См.: Фонд оценочных средств)

Лабораторная работа № 8
«Принципы защиты программно-аппаратным комплексом Dallas Lock»

Форма проведения: **лабораторная работа Цель работы:**

Изучить принципы защиты программно-аппаратным комплексом Dallas Lock.

Одна из важных составляющих работ по обеспечению безопасности информационных систем —защита рабочих станций и серверов от несанкционированного

доступа. И первым рубежом защиты любой компьютерной системы является обеспечение доверенной загрузки вычислительной среды. Для этого существует специальный класс средств — модули доверенной загрузки. Модули доверенной загрузки операционной системы применяются уже более 20 лет, и сегодня этот класс средств защиты не теряет свою актуальность. Продукты этого типа являются «первым эшелоном защиты» вычислительных систем, и именно на них возлагаются задачи контроля доступа пользователей, контроля целостности программной среды и аппаратных ресурсов компьютерной системы.

Необходимость применения средств доверенной загрузки также отражена и в нормативных документах ФСТЭК России — согласно Приказам № 17 и 21, в государственных информационных системах 1 и 2 классов и в информационных системах персональных данных, при необходимости обеспечения 2 и выше уровня защищенности персональных данных, данная мера является базовой.

Рисунок 1. Средство доверенной загрузки Dallas Lock

Средство доверенной загрузки Dallas Lock Системные требования и поддерживаемые технологии Средство доверенной загрузки Dallas Lock предназначено для защиты от несанкционированного доступа компьютеров архитектуры Intel x86 и может быть реализовано на различных платах, предназначенных для работы с разными шинными интерфейсами вычислительной техники: PCI Express, Mini PCI Express, M.2.

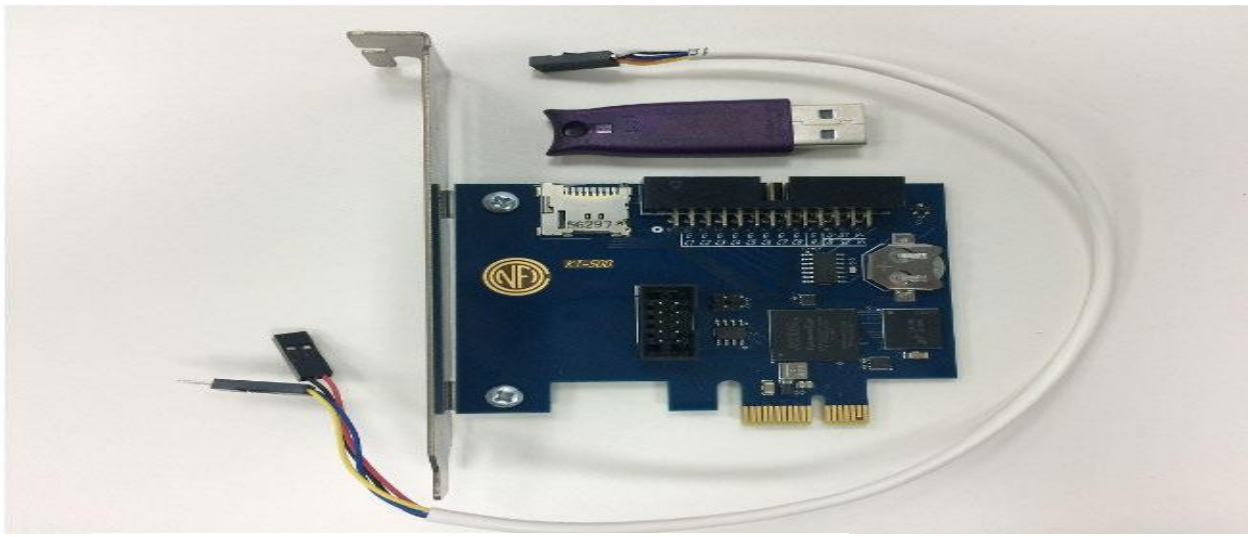


Рисунок 2. Плата СДЗ Dallas Lock формата PCI Express

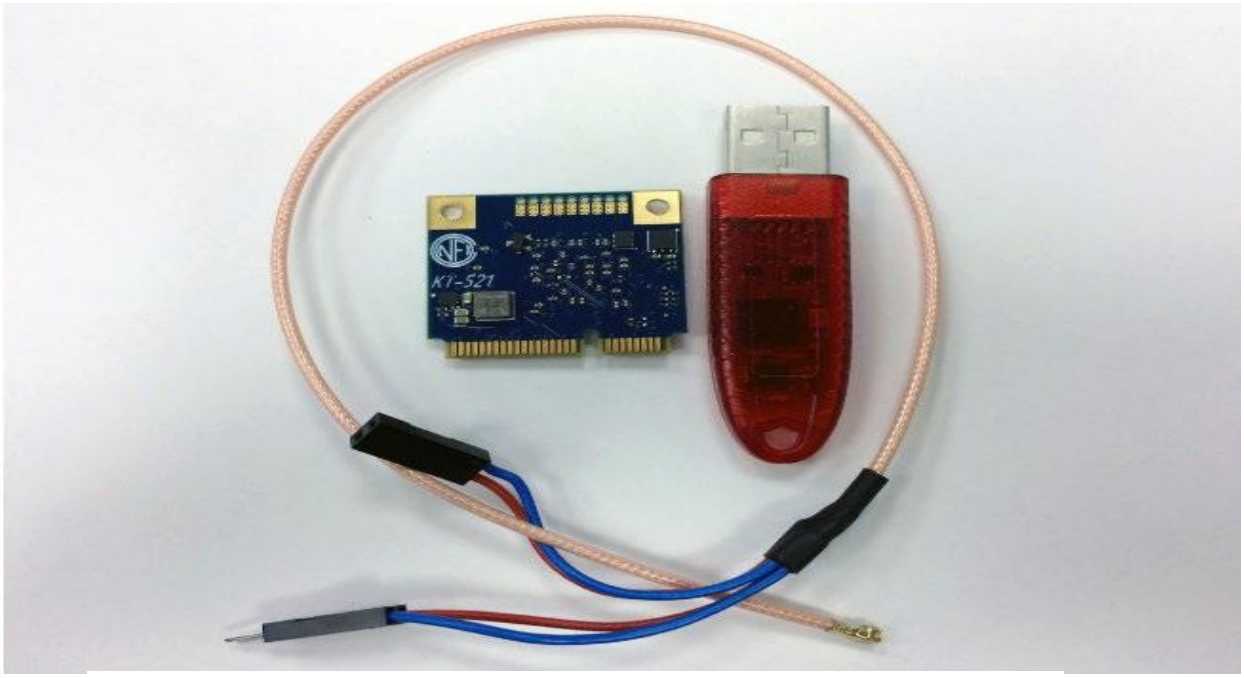


Рисунок 3. Плата СДЗ Dallas Lock формата Mini PCI Express (Half Size)

Рисунок 4. Плата СДЗ Dallas Lock формата M.2

Плату PCI Express можно применить как с полнопрофильной планкой, так и низкопрофильной, что дает возможность использования в разных корпусах. Допускается подключать плату PCI Express к разъему PCI через переходник. СДЗ в форм-факторе M.2 имеет размер 22мм x 30мм, что позволяет обеспечивать доверенную загрузку современных ноутбуков и моноблоков. В разъем M.2 допускается вставлять различные по размеру устройства. Например, устройства Mini PCI Express можно подключать к разъему M.2 через переходник, но в подавляющем большинстве случаев именно совокупный размер (вместе с переходником) является ограничением для применения такого решения в современных ноутбуках и моноблоках. В плате M.2 это ограничение отсутствует.

Особенных требований СДЗ Dallas Lock не предъявляет — минимальная и оптимальная конфигурация компьютера в большей степени определяется требованиями операционной системы. Минимальные аппаратные требования к вычислительной технике для установки СДЗ Dallas Lock следующие: Процессор Pentium с частотой от 300 МГц. Не менее 128 МБ оперативной памяти. Свободный разъем PCI Express / Mini PCI Express на материнской плате для подключения СДЗ. Разъем Reset для подключения сторожевого таймера СДЗ. Наличие свободных портов USB для использования аппаратных идентификаторов. Клавиатура и компьютерная мышь. Видеоадаптер и монитор, поддерживающие режим Super VGA, с разрешением не менее чем 800x600 точек. Компьютеры могут иметь в своем составе системные платы как с BIOS, так и UEFI. В СДЗ Dallas Lock реализована поддержка наиболее распространенных файловых систем, включая: FAT12, FAT16, FAT32, NTFS, Ext2, Ext3, Ext4, VMFS. При этом для СДЗ Dallas Lock не важно, какая операционная система установлена на компьютере. Значение имеет только файловая система. Кроме того, СДЗ Dallas Lock поддерживает широкий перечень аппаратных идентификаторов: USB-ключи Aladdin eToken Pro/Java1; USB-ключи Рутокен; электронные ключи Touch Memory (iButton); USB-ключи JaCarta (JaCarta ГОСТ, JaCarta PKI); аппаратные идентификаторы ESMART (смарт-карты: ESMART Token ГОСТ, ESMART Token SC 64K; USB-токены: ESMART Token ГОСТ, ESMART Token USB 64K). Также стоит отметить, что при использовании СДЗ Dallas Lock аппаратная идентификация не является обязательной — можно использовать для входа логин, вводимый с клавиатуры. Функциональные возможности СДЗ Dallas Lock К основным функциональным возможностям СДЗ Dallas Lock относятся: идентификация и аутентификация пользователя до выполнения действий по загрузке операционной системы или администратора до выполнения действий по управлению СДЗ; двухфакторная аутентификация пользователей при совместном использовании СДЗ с аппаратными идентификаторами; контроль целостности загружаемой операционной системы, блокирование загрузки операционной системы при нарушении целостности загружаемой программной среды (операционной системы); блокирование загрузки операционной системы при выявлении попыток загрузки нештатной операционной системы; блокировка пользователя при выявлении попыток обхода СДЗ; автоматическая регистрация событий, относящихся к безопасности компьютера и СДЗ, в соответствующих журналах аудита. Предоставляет возможность защиты от несанкционированного уничтожения или модификации записей журнала аудита; реагирование на обнаружение событий, указывающих на возможное нарушение безопасности; недоступность ресурсов СДЗ из штатной операционной системы после завершения работы СДЗ; контроль состава компонентов аппаратного обеспечения ПК на основе их идентификационной информации. Блокирует загрузку операционной системы при обнаружении несанкционированного изменения состава аппаратных компонентов СВТ; выполнение перезагрузки ПК при выявлении попыток обхода СДЗ; автоматическое прохождение идентификации и аутентификации в штатной операционной системе после успешного прохождения авторизации и выполнения загрузки с использованием СДЗ. Средство доверенной загрузки Dallas Lock позволяет осуществлять контроль целостности следующих типов объектов: Файловая система. Реестр ОС Windows. Области диска. BIOS/ CMOS. Аппаратная конфигурация. Соответствие требованиям регуляторов Средство доверенной загрузки Dallas Lock сертифицировано ФСТЭК России на соответствие требованиям к средствам доверенной загрузки по 2 классу защиты в соответствии с профилем защиты ИТ.СДЗ.ПР2.ПЗ и по 2 уровню контроля отсутствия недекларированных возможностей (НДВ) (Сертификат ФСТЭК России № 3666 от 25 ноября 2016 года). Таким образом, программно-аппаратный комплекс может использоваться для защиты государственных информационных систем и АСУ ТП до класса К1, защиты персональных данных до УЗ1, автоматизированных систем до класса 1Б включительно (государственная тайна с грифом «Совершенно секретно»). Работа с

продуктом Инсталляция платы СДЗ Dallas Lock в системный блок осуществляется просто и быстро — плата вставляется в свободный слот PCI Express (Mini PCI Express, M.2), «сторожевой таймер» подключается к разъему Reset. Установка дополнительных программных модулей (агентов) в среду штатной ОС для СДЗ Dallas Lock не требуется. Возможно также использование датчика вскрытия корпуса системного блока. Для этого на плате формата PCIe (КТ-500) имеются входы S1 и S2. При загрузке компьютера с установленной платой появляется экран приглашения войти в систему. Пользователю необходимо ввести логин и пароль и при необходимости предъявить аппаратный идентификатор, если администратор установил данную опцию.

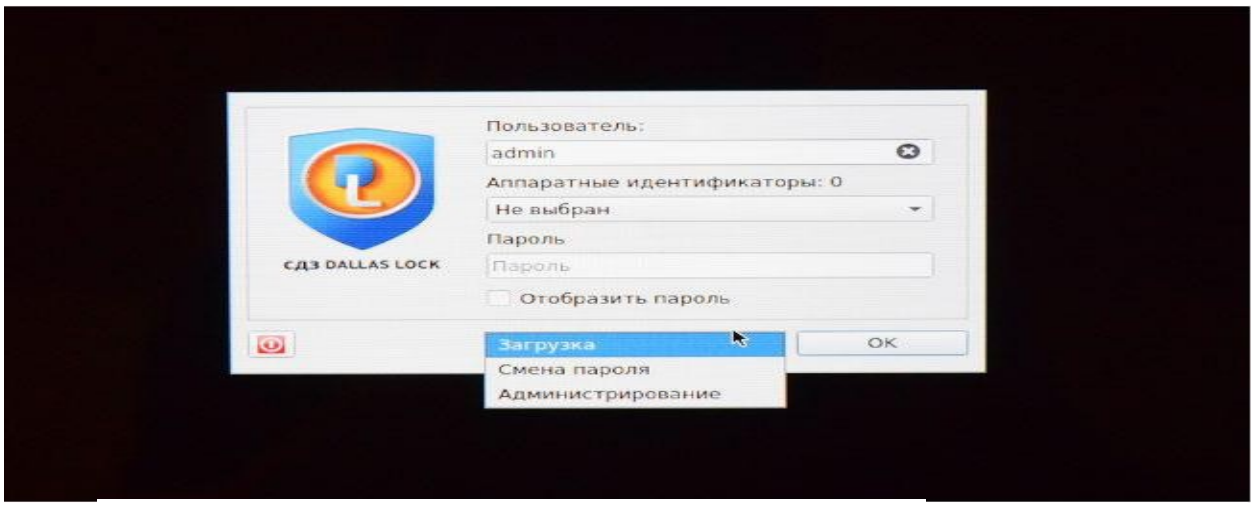


Рисунок 5. Аутентификация пользователя в СДЗ Dallas Lock

В меню в нижней части экрана пользователю можно выбрать следующие действия с системой: «Загрузка» — переход к загрузке штатной операционной системы. «Смена пароля» — переход к смене пароля текущей учетной записи пользователя. «Администрирование» — запуск консоли администратора СДЗ Dallas Lock, которая доступна только пользователям с ролью «Администратор» и «Аудитор». После успешной авторизации пользователя происходит переход к процедуре контроля целостности объектов. При успешном ее прохождении выводится соответствующее сообщение. При входе пользователей с полномочиями аудитора или администратора в окне контроля целостности помимо результата отображается ход выполнения процедуры контроля целостности объектов.

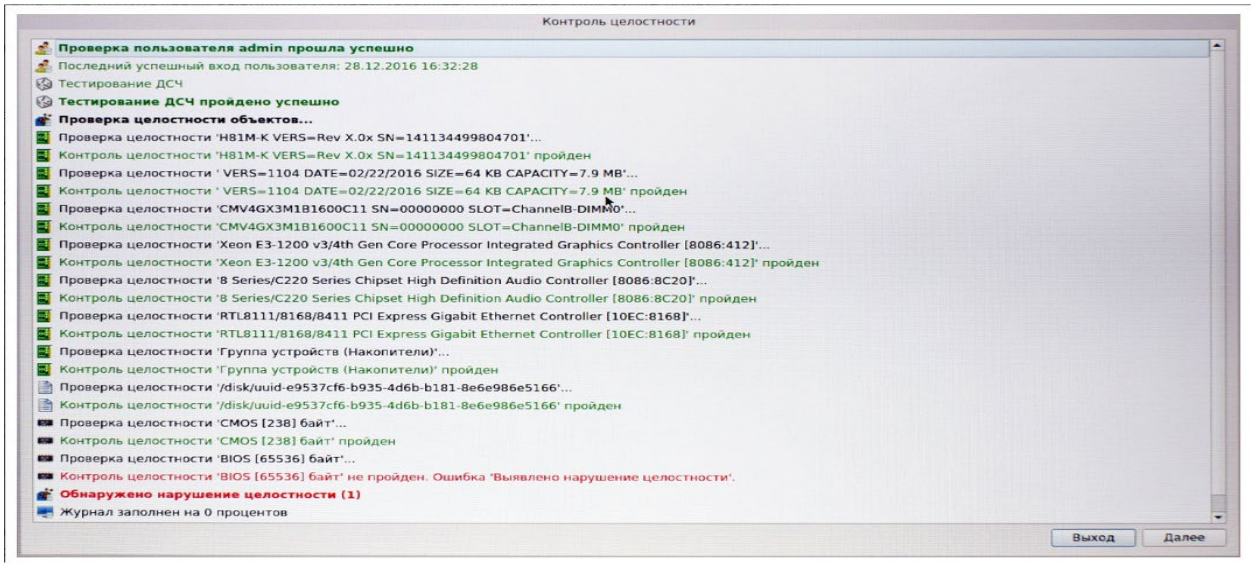


Рисунок 6. Сообщение о неуспешном прохождении контроля целостности в СДЗ Dallas Lock

В главном окне консоли администратора расположены вкладки, обеспечивающие доступ к различным настройкам СДЗ Dallas Lock: «Пользователи» — управление учетными записями пользователей. «Контролируемые объекты» — контроль целостности компонентов СВТ. «Политики безопасности» — настройка авторизации в СДЗ Dallas Lock. «Журнал» — регистрация и аудит. «Параметры» — управление параметрами платы. «Сервис» — дополнительные функции СДЗ Dallas Lock. Отметим, что разработчик при проектировании интерфейса всех своих продуктов использует унифицированный дизайн. Это позволяет пользователям других продуктов линейки Dallas Lock легко осваивать новые продукты, не тратя время на дополнительное обучение.

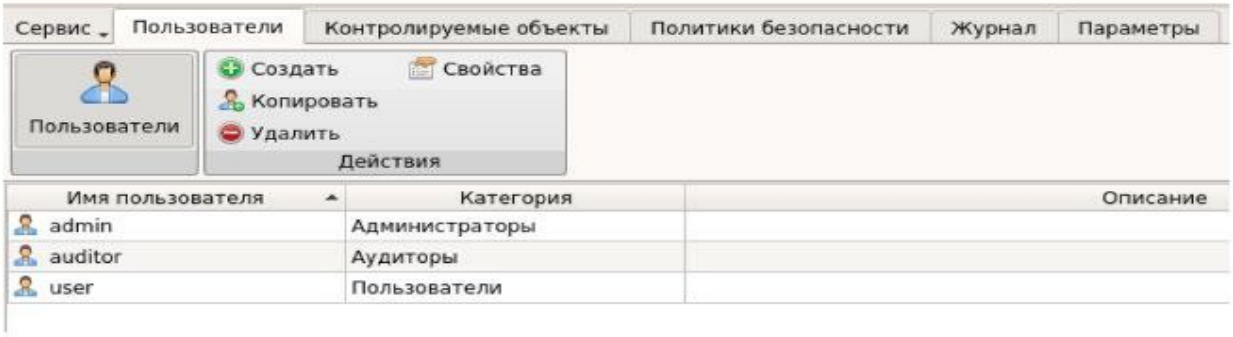


Рисунок 7. Меню «Пользователи» в консоли администратора СДЗ Dallas Lock

Во вкладке «Пользователи» учетные записи пользователей, которые зарегистрированы в СДЗ Dallas Lock, отображаются в виде таблицы. Если учетная запись пользователя отключена или заблокирована, то в списке это обозначается соответствующей иконкой. Администратор имеет возможность формировать и управлять списком учетных записей пользователей СДЗ Dallas Lock, а также производить необходимые настройки политик безопасности, а именно политик авторизации и политик паролей. При этом все операции по управлению учетными записями пользователей фиксируются в журнале.

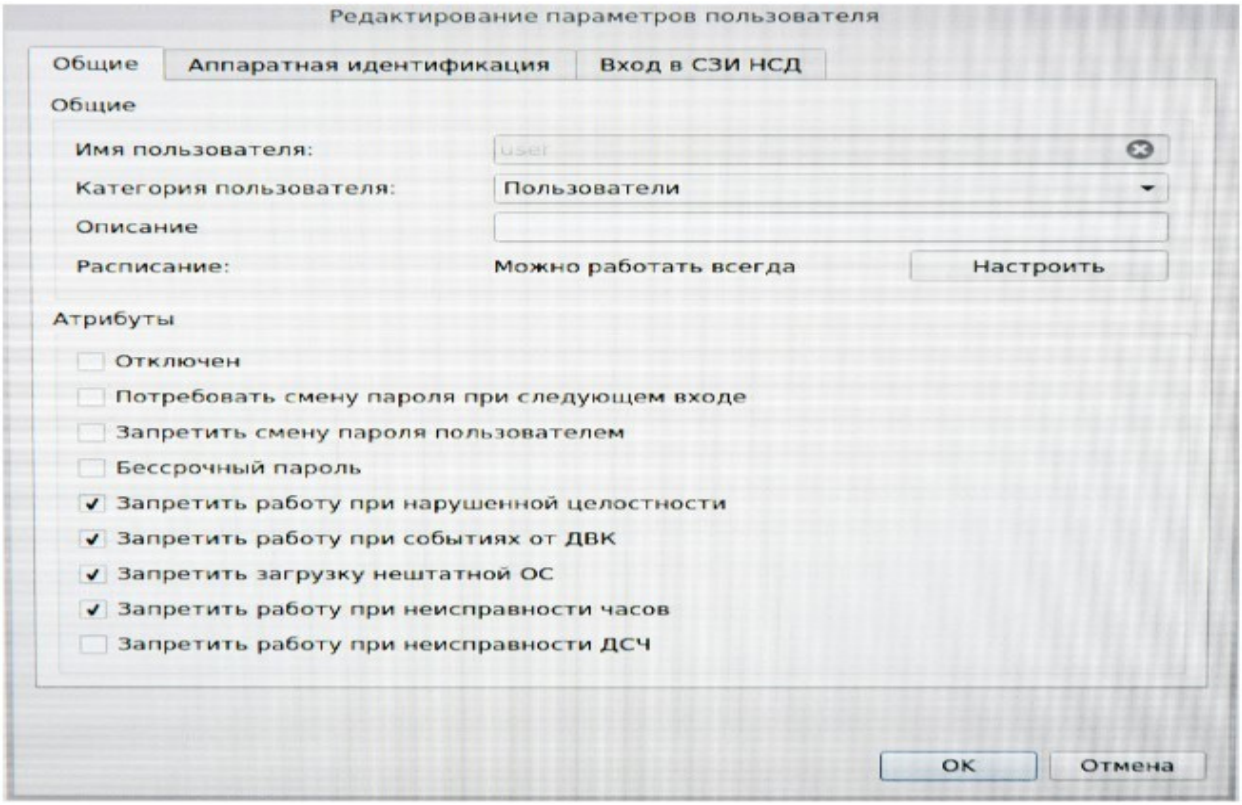


Рисунок 8. Редактирование параметров пользователя в СДЗ Dallas Lock

В параметрах каждого пользователя можно изменить роль, текстовое описание учетной записи, установить разрешенное время для входа в систему и различные атрибуты.

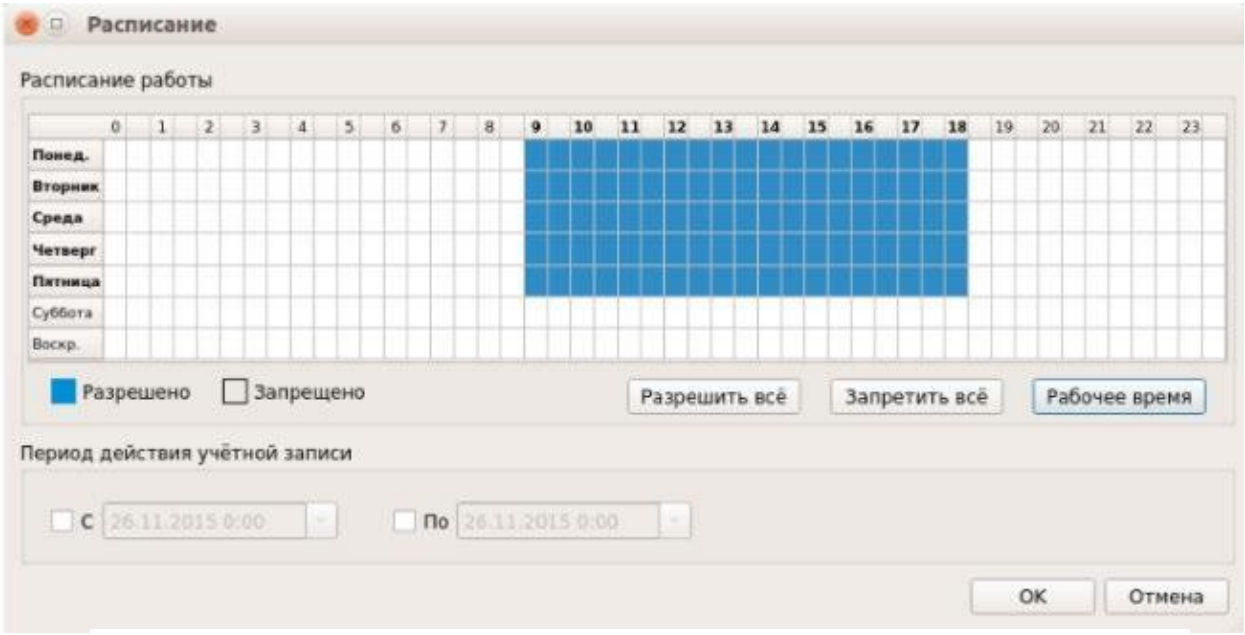


Рисунок 9. Установка разрешенного времени входа в систему в СДЗ Dallas Lock

В разделе «Аппаратная идентификация» пользователю можно назначить аппаратный идентификатор, а в меню «Вход в СЗИ НСД» дополнительно можно настроить автовход в СЗИ от НСД Dallas Lock, установив соответствующий атрибут.

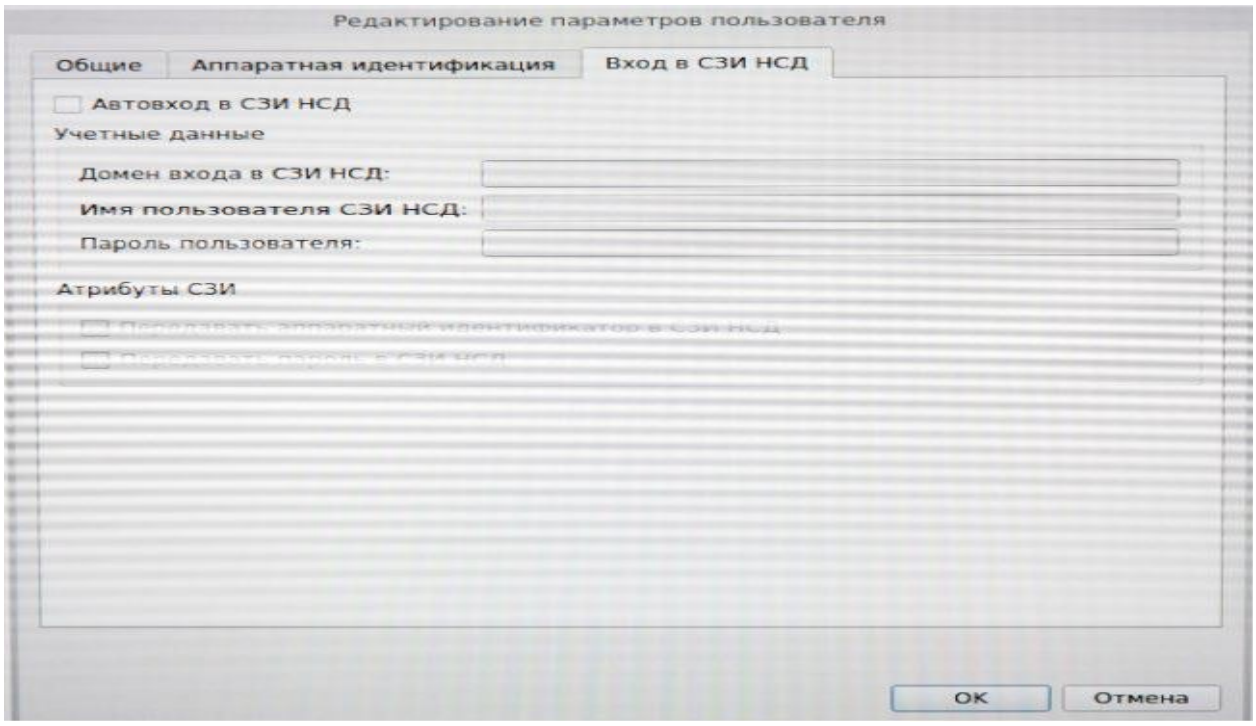


Рисунок 10. Вкладка «Вход в СЗИ НСД» в СДЗ Dallas Lock

Как мы уже ранее указывали, СДЗ Dallas Lock позволяет осуществлять контроль целостности следующих типов объектов: Файловая система. Реестр ОС Windows. Области диска. BIOS/CMOS. Аппаратная конфигурация. Для контроля целостности объектов файловой системы, реестра и областей диска используется метод сравнения расчетной контрольной суммы (КС), полученной в момент проверки целостности, с эталонной контрольной суммой, рассчитанной в момент назначения целостности. Для подсчета

контрольных сумм используются алгоритмы CRC32, хэш MD5, хэш ГОСТ Р 34.11-94. Контроль целостности остальных объектов осуществляется методом полной сверки. Просмотр контролируемых объектов конкретной категории осуществляется через соответствующие кнопки в панели «Категория», а добавление и редактирование в панели «Действия».

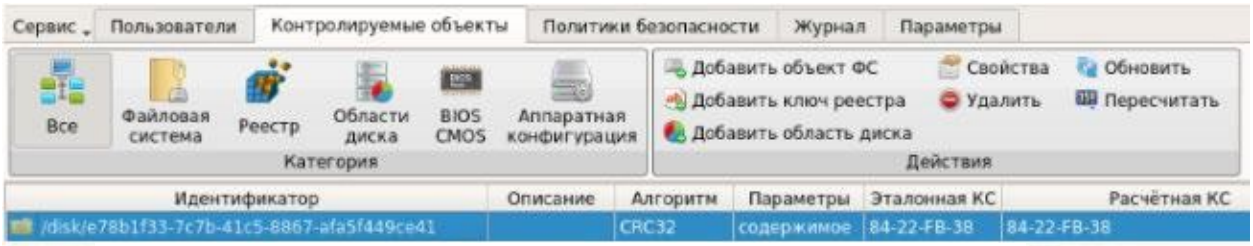


Рисунок 11. Просмотр контролируемых объектов в СДЗ Dallas Lock

Для контроля целостности объектов файловой системы необходимо задать путь к файлу или каталогу (директории) контролируемого объекта, выбрать алгоритм расчета и установить дополнительные необходимые атрибуты. Для объектов реестра Windows выбирается путь к файлу реестра и путь к контролируемому объекту в указанном выше файле реестра, а также алгоритм расчета контрольных сумм и дополнительные атрибуты контроля. Для контроля целостности областей жесткого диска задаются начальный сектор и количество секторов, подлежащих контролю. Для категории BIOS/CMOS форма просмотра разделена на два блока — BIOS и CMOS, представляющие две таблицы значений, где цветом можно выделять ячейки, для которых нужно назначить контроль, установив соответствующие чекбоксы.

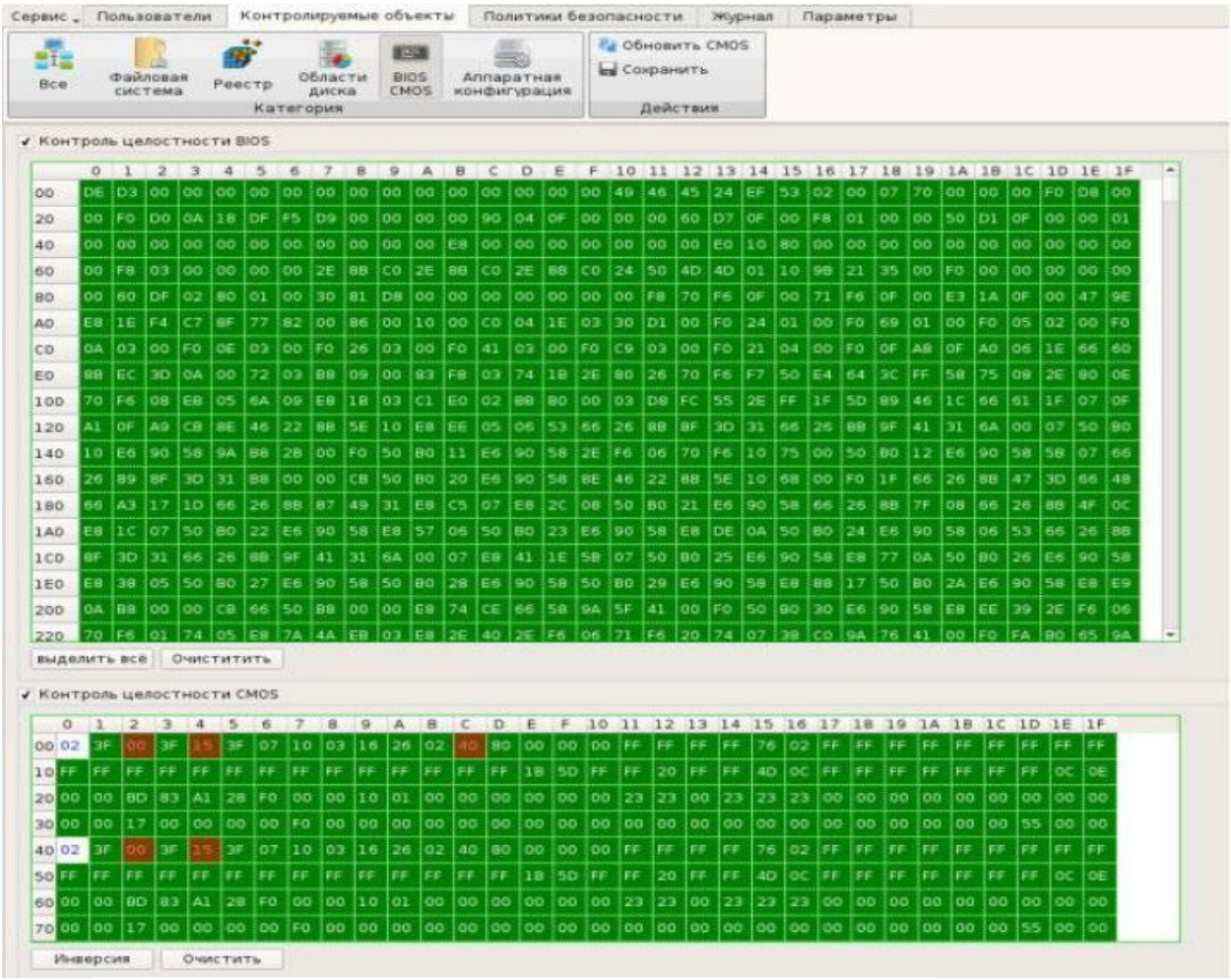


Рисунок 12. Параметры контроля BIOS/CMOS в СДЗ Dallas Lock

В списке объектов аппаратной конфигурации автоматически отображаются все аппаратные устройства, установленные на компьютере. Для настройки контроля аппаратной конфигурации в основной области доступны чекбоксы, соответствующие группам, — «Контролировать группу» и «Включить/исключить из контроля целостности» (напротив конкретного идентификатора в группе). Особенность реализации контроля целостности аппаратной конфигурации заключается в алгоритме исключения устройства из-под контроля. В этом случае фактическое наличие или отсутствие такого устройства не будет нарушать целостность конфигурации. Такая реализация позволяет пользователю комфортно работать с различного рода USB-устройствами.

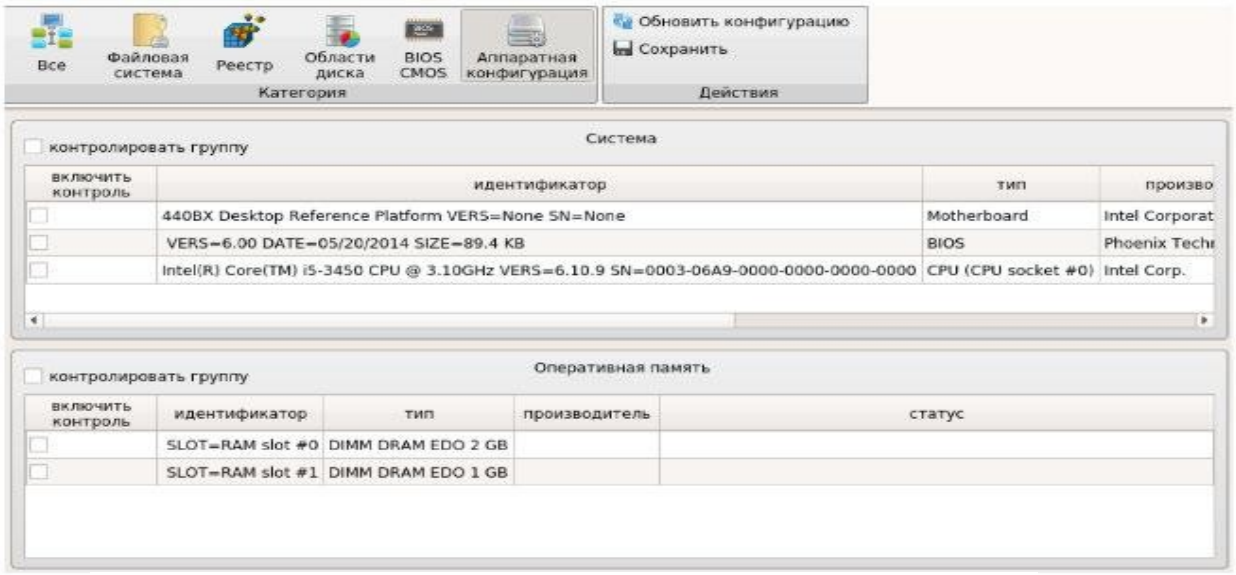


Рисунок 13. Параметры аппаратной конфигурации в СДЗ Dallas Lock

Для категории «Аппаратная конфигурация» выводятся следующие списки групп: Система — отображается информация о материнской плате, BIOS и ЦП. Оперативная память — отображаются установленные модули оперативной памяти. PCI-устройства — отображаются подключенные PCI-устройства. Накопители — отображаются установленные накопители. USB-устройства — отображаются различные устройства, подключенные через USB-порт. Во вкладке «Политики безопасности» в виде таблицы отображаются параметры и значения политик безопасности. Выделяются следующие категории политик — «Политики авторизации» и «Политики паролей».

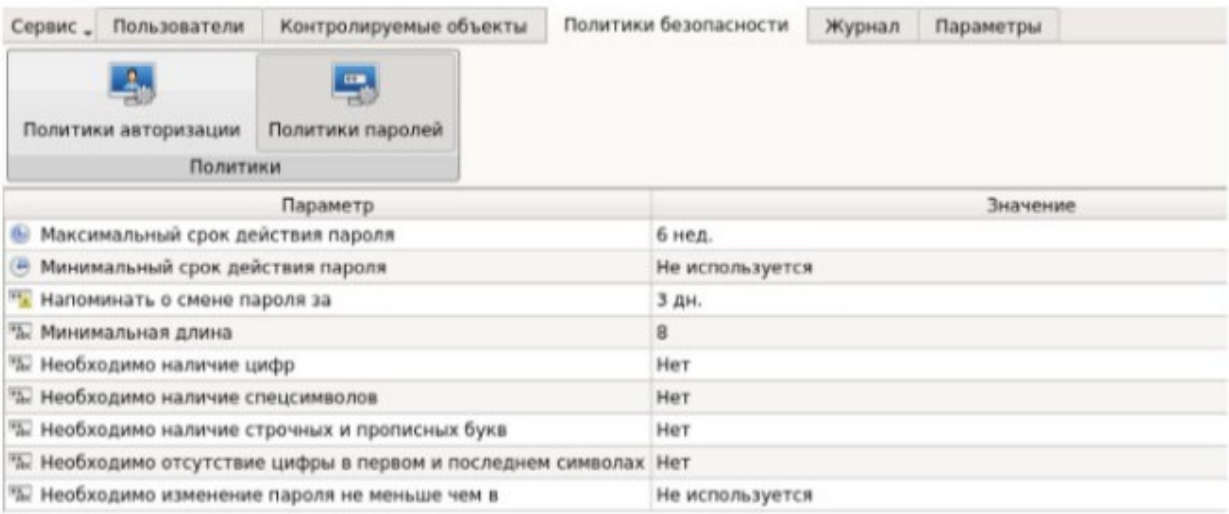


Рисунок 14. Политики паролей в СДЗ Dallas Lock

Просмотр параметров и значений конкретной категории политик осуществляется через соответствующие кнопки в панели «Политики».

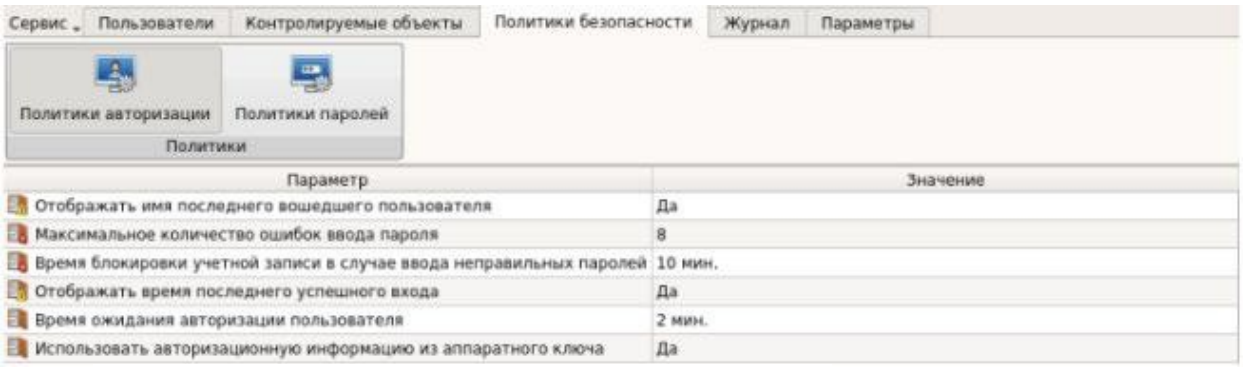


Рисунок 15. Политики авторизации в СДЗ Dallas Lock

Все события, связанные с администрированием СДЗ Dallas Lock, а также события входов пользователей, события проверки целостности и редактирования учетных записей пользователей фиксируются в журнале безопасности. Отображаются все события во вкладке «Журнал» в виде таблицы. Предусмотрена фильтрация записей журнала и их сортировка по порядковому номеру, времени события, пользователям, в течение работы которых произошло событие, наименованию события, результату и описанию (по возрастанию/убыванию). Кроме того, возможен экспорт записей журналов в файл.

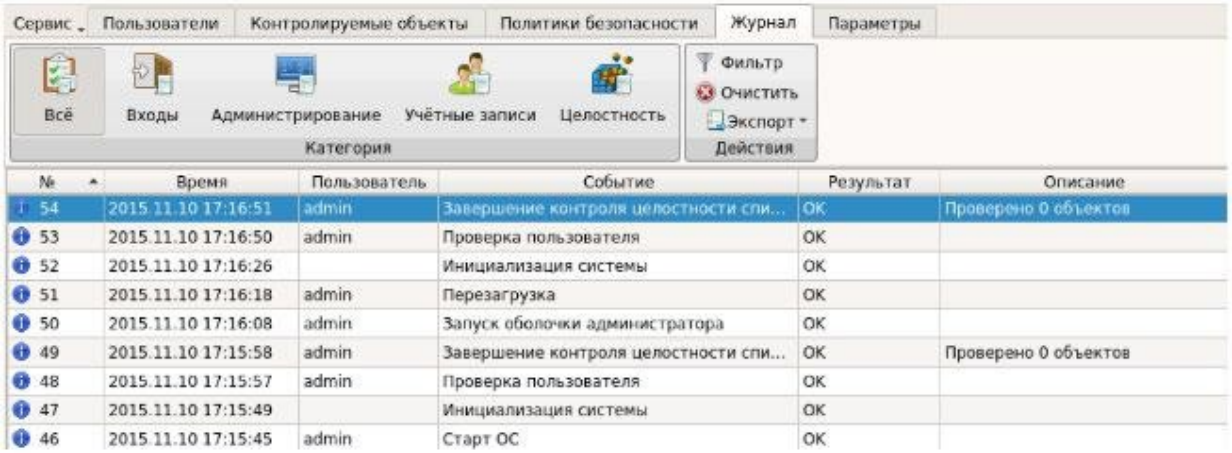


Рисунок 16. Вкладка «Журнал» в СДЗ Dallas Lock

Во вкладке «Параметры» отображается версия СДЗ Dallas Lock и информация о плате, а также настраиваются параметры «Часы», «Загрузочное устройство» (с которого будет загружаться штатная операционная система) и «Датчики вскрытия корпуса». Также в панели «Версия» доступно обновление прошивки. Меню «Сервис» позволяет получить доступ к дополнительным функциям СДЗ Dallas Lock: сохранить параметры конфигурации комплекса (в формате .xml) на различные носители, сохранить отчет о конфигурации СДЗ Dallas Lock в формате .rtf или .html, восстановить конфигурации СДЗ Dallas Lock по умолчанию и выполнить обновление прошивки.

Преимущества: Полная поддержка Unified Extensible Firmware Interface (UEFI). Широкий модельный ряд устройств, включая плату, поддерживающую разъем M.2. Наличие сертификата соответствия новым требованиям ФСТЭК России к средствам доверенной загрузки. Поддержка широкого спектра аппаратных идентификаторов. Поддержка наиболее распространенных файловых систем. Возможность сохранения (восстановления) параметров конфигурации СДЗ на различные носители информации. Наличие датчика вскрытия корпуса. Современный графический интерфейс, исполненный в едином стиле с другими продуктами в линейке Dallas Lock.

Недостатки: Отсутствие централизованного управления средствами доверенной загрузки. Отсутствие в модельном ряду решения для защиты компьютерных систем, в которых нет разъемов для подключения плат расширения. Практическая часть

1. Установить программу
2. Изучить системные требования и поддерживаемые технологии
3. Изучить функциональные возможности
4. Изучить соответствие требованиям регуляторов.
5. Сделать выводы.

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы
1-2	1-2	1-2	1-4

Оценочные средства: отчет к лабораторной работе (См.: Фонд оценочных средств)

Лабораторная работа № 9
«Освоение принципов документального оформления структуры и работы защищенных (Digital Security Office)»

Форма проведения: **лабораторная работа**

Цель работы:

Целью данной лабораторной работы является изучение принципов документального оформления структуры и работы защищенных (Digital Security Office)».

Digital Security Office 2006 - законченное решение для комплексного управления информационной безопасностью компании. **Digital Security Office 2006** включает в себя систему анализа и управления информационными рисками **ГРИФ** и систему разработки и управления политикой безопасности информационной системы **КОНДОР**. С помощью программы **КОНДОР** проводится аудит ИС компании на соответствие стандарту ISO 17799. На основе данных, полученных в результате проведения аудита, разрабатывается политика безопасности компании и система управления информационной безопасностью [8].

Operationally Critical Threat, Asset, and Vulnerability Evaluation^{SM} (OCTAVE) [9]

OCTAVE - это метод выявления и оценки угроз, уязвимостей, рисков и мер по их устранению на предприятии. Метод основан на ряде критериев, которые определяют основные источники рисков для самостоятельной их оценки и принятия мер по их устранению. Несмотря на то, что это метод самостоятельной оценки безопасности информационных технологий, он также допускает использование экспертов для проведения конкретных мероприятий, в случае необходимости. OCTAVE представляет собой набор документов с руководством по внедрению данного метода. Руководство состоит из 18 частей и включает в себя: подробное описание метода, рекомендации по подбору и подготовке персонала, руководство по оценке и рисков, и методов их устранения, описание всевозможных информационных потоков на предприятии.

OCTAVE-метод использует трехэтапный подход для рассмотрения организационных и технологических вопросов защиты ИБ, создавая полную картину ИБ организации и её потребностей. При использовании данного метода используются семинары и приветствуется открытое обсуждение и обмен информацией об угрозах, совместная выработка стратегии их устранения. Каждый этап состоит из нескольких

процессов, каждый процесс включает в себя один или несколько рабочих совещаний, проводимых группой аналитиков.

Рассмотренные подходы к моделированию АС и процесса обеспечения информационной безопасности разрабатывались с целью выявления угроз безопасности информации в АС, оценки рисков и выработки методов нейтрализации этих угроз. Однако основной целью данной работы является моделирование непосредственно самого процесса защиты информации. Т.е. формирование неких событий, негативно влияющих на защищенность информации в АС, предложение пользователю возможных решений по нейтрализации данного воздействия и оценки выработанного им решения. Одним из методов, которые можно использовать для моделирования объекта защиты, является метод, предложенный в статье В. В. Золотарева, Е. А. Даниловой [5]. Этот метод предполагает разбиение АС на следующие структурные элементы: ОМ - организационные меры защиты информации, ТС - технические средства, ПО - программное обеспечение, Ч - человеческий фактор. Также предполагается, что каждый элемент системы может находиться в одном из следующих состояний: Отк - отказ, О - ошибка, С - сбой, Р - работоспособное состояние. Все подсистемы и состояние представляются в виде матрицы (рис.1), в которой впоследствии исключаются невозможные либо не влияющие на защищенность информации состояния.

		ТС				ПО				ОМ				Ч			
		Р	О	С	Отк	Р	О	С	Отк	Р	О	С	Отк	Р	О	С	Отк
ТС	Р																
	О																
	С																
	Отк																
ПО	Р																
	О																
	С																
	Отк																
ОМ	Р																
	О																
	С																
	Отк																
Ч	Р																
	О																
	С																
	Отк																

Рисунок 1. Матричное представление декомпозиции факторов

Данная матрица отражает взаимодействие различных элементов системы в зависимости от их состояний, но сами состояния заданы в общем виде (например, рассматривается взаимодействие любого ПО с любыми ТС), поэтому для увеличения комбинаций этих состояний можно разделить (конкретизировать) предложенные элементы системы (ПО, ТС, МО и Ч) и рассмотреть их взаимодействие. Это существенно расширит количество состояний и вариантов их взаимодействия и поможет исключить некоторые невозможные взаимосвязи. В рамках поставленной задачи было принято следующее деление.

Организационные меры:

- меры, направленные на сотрудников организации (включают в себя подбор, проверку, инструктаж сотрудников);
- меры, направленные на защиту информации от лиц, не являющихся сотрудниками организации, но имеющих потенциальную возможность нанести вред защищаемой информации (напр., обеспечению режима физической охраны объектов).

Человеческий фактор:

- персонал, работающий с защищаемой информацией (напр., бухгалтера, директор);
- персонал, обеспечивающий защищенность информации (напр., системный администратор, охранники).

Данное деление выбрано с учетом мер, которые специалист по защите информации может применять к той или иной группе персонала в процессе деятельности. Т.е. по отношению к персоналу, работающему с защищаемой информацией, список мер ограничивается инструктажем и проверкой их деятельности, в то время как меры по отношению ко второй группе персонала расширятся до сокращения или увеличения штата тех или иных сотрудников, принадлежащих к этой группе.

Программное обеспечение:

- участвующее в обработке защищаемой информации;
- обеспечивающее безопасность хранения и передачи защищаемой информации.

Технические средства:

- зависимые от ПО (напр., компьютеры на рабочих местах, серверы);
- независимые от ПО (напр., энергоснабжения).

При таком делении ОМ напрямую могут взаимодействовать только с персоналом (Ч). Персонал в свою очередь может оказывать влияния как на ТС, так и на ПО. Также ТС и ПО могут взаимодействовать между собой, но ПО может влиять только на определенную группу ТС. Для наглядности отразим это на следующей схеме (рисунок 2).

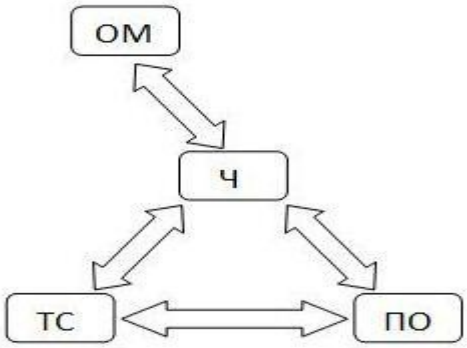


Рисунок 2. Схема взаимодействия элементов автоматизированной системы

Определив все виды взаимодействия элементов системы, можно составить развернутые матричные представления факторов аналогично с представлением представленным выше.

После выбора и описания всех возможных состояний элементов АС, негативно влияющих на защищенность информации, необходимо количественно оценить их влияние, выработать порядок генерации данных состояний, описать возможные меры по противодействию данным влияниям и их количественную оценку, выбрать методы оценки эффективности действий пользователя.

Для оценки количественного влияния факторов, негативно влияющих на защищенность информации, и мер противодействия можно прибегнуть к требованиям стандартов и экспертным оценкам [6]. Стоит отметить, что на данной стадии будут закладываться те навыки и принципы, которые приобретет и которыми будет руководствоваться человек, прошедший обучение по данной методике, поэтому от грамотной настройки количественных показателей будет во многом зависеть эффективность обучения. Кроме того, не стоит забывать, что модель должна соответствовать реальному объекту, а на практике воздействие одного и того же негативного фактора может иметь различную критичность. Поэтому количественное влияние для негативных факторов не должно быть фиксированным (в то время как меры

противодействия как раз наоборот должны иметь постоянное значение), а скорее носить случайный характер, но иметь некоторое среднее. Это усилит уровень детализации модели, но значительно усложнит оценку пользовательского решения. Также количественное влияние должно быть представлено в таком виде, в котором пользователь сможет визуально оценить угрозу как отдельного фактора, так и угрозу набора факторов, формирующих ситуацию.

Множество состояний, в которых может находиться объект защиты, описанное выбранной факторной моделью, генерируется путем комбинирования списка факторов и вариации их количественного влияния. Генерацию списка негативных факторов можно проводить случайным образом, но для большего соответствия модели реальному объекту стоит учесть, что факторы не являются равновероятными. Обучаемому необходимо будет каждый раз при использовании данного программного комплекса формировать комплекс мер в соответствии со своими теоретическими знаниями для максимально эффективного устранения предложенных угроз. Анализируя результат каждого решения, пользователь сможет делать выводы об эффективности его реакций на предложенную ситуацию.

Также немаловажную роль будет иметь и само описание факторов. Рассмотренное ранее представление факторов формализует их описание, что может негативно сказаться на эффективности обучения. Частично решить эту проблему можно путем составления списка элементов каждой подсистемы (напр., в программное обеспечение могут входить: ОС, брандмауэры, антивирусы, офисное ПО и т.д.). Для описания и расширения списка факторов стоит рассмотреть и существующие стандарты в области информационной безопасности (таких как ГОСТ Р ИСО/МЭК 15408-2002).

Отдельного внимания также заслуживает список мер по нейтрализации негативного воздействия на защищенность информации, в котором основным показателем эффективности принятых мер будет их стоимость. Но далеко не все меры имеют стоимость. Существует ряд мер, таких как инструктаж, почтовая рассылка и т.п., которые не будут иметь стоимости. Очевидно, что в таком случае они будут наиболее эффективными, и для каждой сгенерированной ситуации можно будет применять сначала все возможные меры с нулевой стоимостью, вне зависимости от самой ситуации и значений факторов. Чтобы избежать подобных тривиальных решений, список мер для каждой задачи можно ограничить в зависимости от количества сгенерированных факторов и бесплатных мер, которые будут иметь эффект в данной ситуации. Такое ограничение не противоречит "поведению" реального объекта защиты, а скорее, наоборот, может быть интерпретировано тем, что данные меры требуют физических и временных затрат, что, опять же, позволяет улучшить соответствие автоматизированной системы и разработанной модели.

С учетом описанных выше свойств параметров модели необходимо, чтобы программная реализация имела возможность хранения больших объемов многомерных данных и их связей, а также возможность редактирования списка негативных факторов, мер противодействия и настройки их количественных показателей напрямую, без изменения программного кода. Реализовать эти требования можно, используя при разработке базы данных, представив все данные в виде трех таблиц:

1. список негативных факторов и диапазона значений их критичности;
2. список мер по нейтрализации негативного воздействия с указанием их количественного влияния;
3. вспомогательная таблица для хранения списка элементов автоматизированной системы.

Общую схему взаимодействия таблиц можно представить следующим образом (рис.3).

Рисунок 3. Схема взаимодействия таблиц

Так как целью данной работы является не точное моделирование процесса обеспечения информационной безопасности в конкретной АС, а обучение и проверка навыков специалиста по защите информации, при проектировании можно делать акцент на различные принципы защиты информации в АС (как наиболее общие, так и свойственные какому-либо классу АС, или вообще моделировать точно определенный объект защиты). Ситуации также можно задавать заранее или использовать случайный порядок генерации.

С учетом сформированных требований и выбранных методов было разработано программное обеспечение. Ниже приведен его интерфейс (рисунок 4).

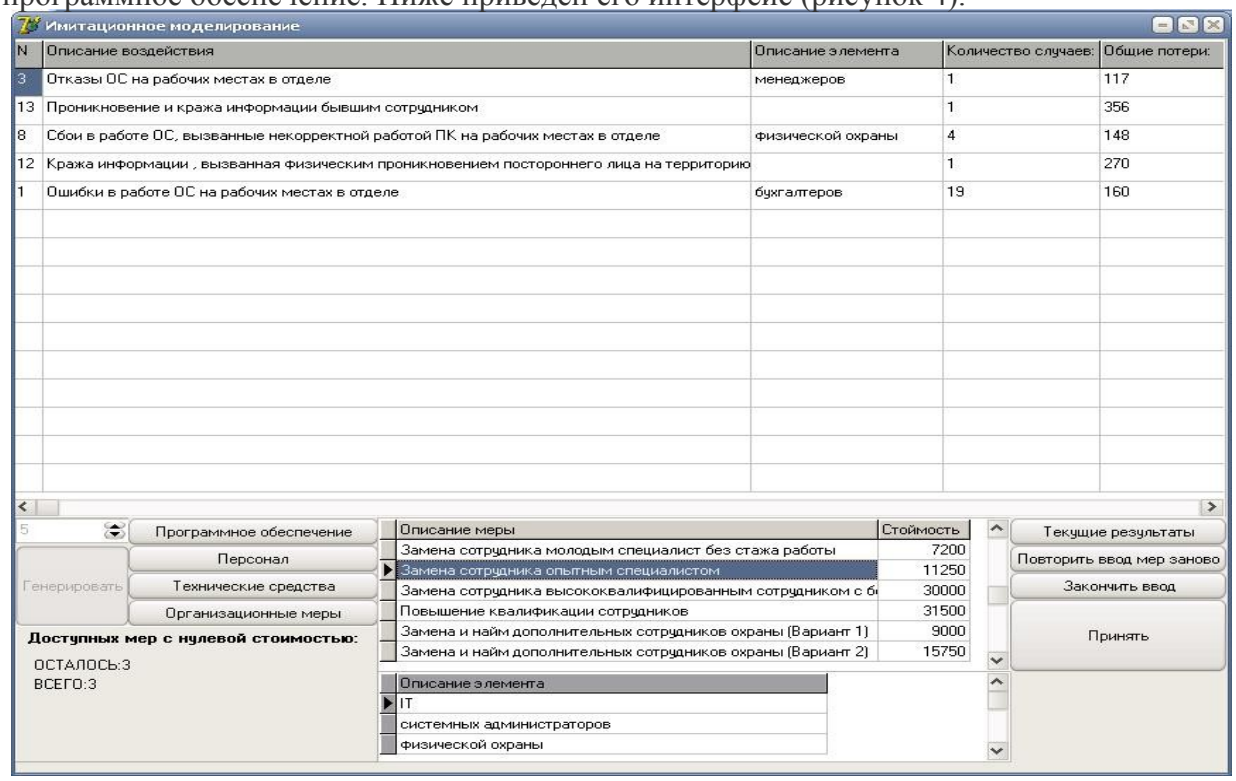


Рисунок 4. Интерфейс программного обеспечения

1. Установить систему Digital Security Office
2. Произвести первоначальную настройку системы
3. Освоить инструментарий системы
4. На заданном примере АС произвести анализ рисков
5. Разработать Политику безопасности предложенной АС.

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы
1-2	1-2	1-2	1-4

Оценочные средства: отчет к лабораторной работе (См.: Фонд оценочных средств)

8. КРИТЕРИИ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ

Оценка «отлично» выставляется студенту, если он продемонстрировал глубокие, исчерпывающие знания и творческие способности в понимании, изложении и использовании учебно-программного материала; логически последовательные, содержательные, полные, правильные и конкретные ответы на все поставленные вопросы и дополнительные вопросы преподавателя; свободное владение основной и дополнительной литературой, рекомендованной учебной программой.

Оценка «хорошо» выставляется студенту, если он продемонстрировал твердые и достаточно полные знания всего программного материала, правильное понимание сущности и взаимосвязи рассматриваемых процессов и явлений; последовательные, правильные, конкретные ответы на поставленные вопросы при свободном устранении замечаний по отдельным вопросам; достаточное владение литературой, рекомендованной учебной программой.

Оценка «удовлетворительно» выставляется студенту, если он продемонстрировал твердые знания и понимание основного программного материала; правильные, без грубых ошибок ответы на поставленные вопросы при устранении неточностей и несущественных ошибок в освещении отдельных положений при наводящих вопросах преподавателя; недостаточное владение литературой, рекомендованной учебной программой.

Оценка «неудовлетворительно» выставляется студенту, если он продемонстрировал неправильные ответы на основные вопросы, допущены грубые ошибки в ответах, непонимание сущности излагаемых вопросов; неуверенные и неточные ответы на дополнительные вопросы.

9. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ

Текущая аттестация студентов проводится преподавателями, ведущими лабораторные занятия по дисциплине, в следующей форме: отчет письменный по заданию преподавателя.

Допуск к лабораторным работам происходит при наличии у студентов печатного варианта отчета. Защита отчета проходит в форме доклада студента по выполненной работе и ответов на вопросы преподавателя.

Отчет включает в себя следующие разделы: титульный лист с названием работы; цель работы; краткие теоретические сведения; описание результатов лабораторной работы (скриншоты); вывод из работы, включающий в себя описание проделанной работы.

Оценку «отлично» студент получает, если оформление отчета соответсвует установленным требованиям, правильно отвечает на предложенные преподавателем контрольные вопросы, правильно отвечает на дополнительные вопросы по теме

лабораторной работы.

Оценку «хорошо» студент получает, если оформление отчета соответсвует установленным требованиям, правильно отвечает на предложенные преподавателем контрольные вопросы.

Оценку «удовлетворительно» студент получает без беседы с преподавателем, если оформление отчета соответсвует установленным требованиям.

Отчет может быть отправлен на доработку в следующих случаях:

- польностью не соовествует установленным требованиям;
- не раскрыта суть работы.

1. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

10.1. Рекомендуемая литература

10.1.1. Основная литература

1. 1. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ Шаньгин В.Ф.— Электрон. текстовые данные.— М.: ДМК Пресс, 2014.— 702 c.— Режим доступа: http://www.iprbookshop.ru/29257.— ЭБС «IPRbooks»
2. 2. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс]: учебное пособие для вузов/ Девянин П.Н.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2013.— 338 c.— Режим доступа: http://www.iprbookshop.ru/52225.— ЭБС «IPRbooks»

10.1.2. Дополнительная литература:

1. 1. Заика А.А. Локальные сети и интернет [Электронный ресурс]/ Заика А.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 323 c.— Режим доступа: http://www.iprbookshop.ru/52150.— ЭБС «IPRbooks»
2. 2. Инструментальный контроль и защита информации [Электронный ресурс]: учебное пособие/ Н.А. Свинарев [и др.].— Электрон. текстовые данные.— Воронеж: Воронежский государственный университет инженерных технологий, 2013.— 192 c.— Режим доступа: http://www.iprbookshop.ru/47422.— ЭБС «IPRbooks»

10.1.3. Методическая литература:

1. Методические указания по выполнению лабораторных работ по дисциплине «Программно-аппаратные комплексы защиты объектов информатизации»
2. Методические рекомендации для студентов по организации и проведению самостоятельной работы по дисциплине «Программно-аппаратные комплексы защиты объектов информатизации»

10.1.4. Интернет-ресурсы:

1. Университетская библиотека online. http://www.biblioclub.ru.
2. ЭБС «IPRbooks». http://www.iprbookshop.ru.

3. Электронная библиотека СКФУ..http://catalog.ncstu.ru.
4. Государственная публичная научно- техническая библиотека России. (ГПНТБ России). www.gpntb.ru.