РОССИЙСКАЯ ФЕДЕРАЦИЯ МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ ФГАОУ ВО ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ НАУК

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Паюсова. Т. И.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

ТЮМЕНЬ 2021

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Целью дисциплины «Информационные техологии» является обучение студентов основам построения, эксплуатации и администрированию сетевой инфраструктуры.

Задачей курса является освоение:

- принципов построения информационных систем
- принципов обслуживания информационных систем
- концепции содержания информационных систем

Изучение курса основано на следующих дисциплинах: «Организация электронно-вычислительных машин и вычислительных систем», «Технологии и методы программирования», «Современные информационные системы»

В результате изучения дисциплины студенты должны знать:

- классификацию, фундаментальные модели, определения и понятия информационных технологий;
- принципы работы основных сетевых протоколов (DNS, FTP, HTTP);
- алгоритмы организации корпоративных сетей;
- модели разграничения прав доступа;
- принципы работы антивирусного программного обеспечения, межсетевых экранов, беспроводных маршрутизаторов;
- механизмы и основные способы защиты от атак;
- способы борьбы со спамом и нежелательной почтой.

уметь:

- создавать и администрировать веб-сайты;
- настраивать контроллер домена;
- организовывать, настраивать и администрировать корпоративные сети;
- устанавливать централизованную консоль управления антивирусом под ОС Windows Server.

Тема 1. ОСНОВНЫЕ ПОНЯТИЯ

Windows Server – наиболее распространенная операционная система для серверов. Компьютер, на котором установлена такая операционная система, может выполнять роли файлового сервера, сервера службы веб-приложений, сервера терминалов, почтового сервера, сервера удаленного доступа, службы DNS (доменных имен), службы каталогов, сервера потоков мультимедиа и другие.

Windows Server является достаточно быстрой и надежной ОС. Надежность обеспечивает платформа приложений, в которую встроены функции сервера приложений, а также интегрированная среда обеспечивающая доступность и безопасность информации.

Эту ОС достаточно просто развернуть и проводить ее администрирование. Она дает возможность управлять сетью с помощью политик и автоматизации выполнения каких-либо задач.

Для организаций, работающих с важными сетевыми бизнес-приложениями очень важна, служба кластеров, позволяющая объединить несколько серверов. Узлы в кластере взаимно заменяемы. То есть, если один из серверов становится недоступным, обслуживание переходит на другой сервер.

Сегодня многие локальные сети объединены с интрасетями, экстрасетями и веб-узлами. В связи с этим требования к безопасности системы резко возросли. Современные ОС Windows Server тщательно проверяются на наличие слабых мест и точек ошибок. Например, безопасность вычислительной среды обеспечивает общая языковая среда исполнения.

Файловые службы и службы печати позволяют управлять файловыми ресурсами. В то же время сохраняется безопасность и доступ для пользователей. Служба каталогов в Windows Server называется Active Directory. Благодаря этой службе сохраняются сведения о сетевых объектах. Кроме того, Active Directory позволяет администратору быстро найти данную

информацию. Эта служба также упрощает работу по проектированию, развертыванию и управлению каталогами сети. В оптимальной работе Active Directory поможет консоль управления групповыми политиками.

В Windows Server 2012 появилась концепция Dynamic Access Control. Она позволяет управлять доступом к файлам и папкам во всей сети. DAC делает возможным управление доступом на основании любого атрибута или критерия. С помощью этой концепции можно создавать правила доступа к данным, проводящие проверку членства пользователя в тех или иных группах. Эти правила применимы к любому из серверов сети в форме политик. Тем самым создается общая система безопасности.

Вопросы для подготовки

1. ОС Windows Server.
2. Роль DNS.
3. Типы записей.
4. Передача зон.
5. Серверы пересылки.
6. Защита от атак.

Лабораторная работа №1 "Основы построения корпоративных сетей"

Знакомство с сетевым оборудованием. Определения коммутации и маршрутизации. Построение корпоративной сети в Cisco Packet Tracer.

Лабораторная работа №2 "Принципы работы протокола DNS"

Описание протокола DNS. Типы записей DNS пакета. Трансляция адресов. На установленную ОС Windows Server установить роль DNS. Создать запись типа A и выполнить настройку роли.

Тема 2. ФАЙЛОВЫЕ СИСТЕМЫ

Файловая система — это набор спецификаций и соответствующее им программное обеспечение, которые отвечают за создание, уничтожение, организацию, чтение, запись, модификацию и перемещение файловой информации, а также за управление доступом к файлам и за управлением ресурсами, которые используются файлами.

Система управления файлами является основной подсистемой в абсолютном большинстве современных ОС.

С помощью системы управления файлами:

- связываются по данным все системные обрабатывающие программы;
- решаются проблемы централизованного распределения дискового пространства и управления данными;
- предоставляются возможности пользователю по выполнению операций над файлами (создание и т.п.), по обмену данными между файлами и различными устройствами, по защите файлов от несанкционированного доступа.

В некоторых ОС может быть несколько систем управления файлами, что обеспечивает им возможность работать с несколькими файловыми системами.

Термин «файловая система» определяет принципы доступа к данным, организованным в файлы.

Термин «система управления файлами» относится к конкретной реализации файловой системы, т.е. это комплекс программных модулей, обеспечивающих работу с файлами в конкретной ОС.

Для семейства ОС Windows в основном используются файловые системы: VFAT, FAT32, NTFS.

Рассмотрим структуру этих файловых систем.

В файловой системе FAT дисковое пространство любого логического диска делится на две области:

- системную область и
- область данных.

Системная область создается и инициализируется при форматировании, а впоследствии обновляется при манипулировании файловой структурой.

Системная область состоит из следующих компонентов:

- загрузочного сектора, содержащего загрузочную запись (boot record);
- зарезервированных секторов (их может и не быть);
- таблицы размещения файлов (FAT, File Allocation Table);
- корневого каталога (Root directory, ROOT).

Эти компоненты расположены на диске друг за другом.

Область данных содержит файлы и каталоги, подчиненные корневому.

Область данных разбивают на так называемые кластеры. **Кластер** — это один или несколько смежных секторов области данных. С другой стороны, кластер — это минимальная адресуемая единица дисковой памяти, выделяемая файлу. Т.е. файл или каталог занимает целое число кластеров. Для создания и записи на диск нового файла операционная система отводит для него несколько свободных кластеров диска. Эти кластеры не обязательно должны следовать друг за другом. Для каждого файла хранится список всех номеров кластеров, которые предоставлены данному файлу.

Разбиение области данных на кластеры вместо использования секторов позволяет:

- уменьшить размер таблицы FAT;
- уменьшить фрагментацию файлов;
- сокращается длина цепочек файла Þ ускоряется доступ к файлу.

Однако слишком большой размер кластера ведет к неэффективному использованию области данных, особенно в случае большого количества маленьких файлов (ведь на каждый файл теряется в среднем полкластера).

В современных файловых системах (FAT32, HPFS, NTFS) эта проблема решается за счет ограничения размера кластера (максимум 4 Кбайта)

Картой области данных является **Таблица размещения файлов** (File Allocation Table - FAT) Каждый элемент таблицы FAT (12, 16 или 32 бит) соответствует одному кластеру диска и характеризует его состояние: свободен, занят или является сбойным кластером (bad cluster).

- Если кластер распределен какому-либо файлу (т.е., занят), то соответствующий элемент FAT содержит номер следующего кластера файла;
- последний кластер файла отмечается числом в диапазоне FF8h - FFFh (FFF8h - FFFFh);
- если кластер является свободным, он содержит нулевое значение 000h (0000h);
- кластер, непригодный для использования (сбойный), отмечается числом FF7h (FFF7h).

Таким образом, в таблице FAT кластеры, принадлежащие одному файлу, связываются в цепочки.

Таблица размещения файлов хранится сразу после загрузочной записи логического диска, ее точное расположение описано в специальном поле в загрузочном секторе.

Она хранится в двух идентичных экземплярах, которые следуют друг за другом. При разрушении первой копии таблицы используется вторая.

В связи с тем, что FAT используется очень интенсивно при доступе к диску, она обычно загружается в ОП (в буфера ввода/вывода или кэш) и остается там настолько долго, насколько это возможно.

Основной недостаток FAT - медленная работа с файлами. При создании файла работает правило - выделяется первый свободный кластер. Это ведет к фрагментации диска и сложным цепочкам файлов. Отсюда следует замедление работы с файлами.

Для просмотра и редактирования таблицы FAT можно использовать **утилиту Disk Editor.**

Подробная информация о самом файле хранится в другой структуре, которая называется корневым каталогом. Каждый логический диск имеет свой корневой каталог (ROOT, англ. - корень).

Корневой каталог описывает файлы и другие каталоги. Элементом каталога является дескриптор (описатель) файла.

Дескриптор каждого файла и каталога включает его

- имя
- расширение
- дату создания или последней модификации
- время создания или последней модификации
- атрибуты (архивный, атрибут каталога, атрибут тома, системный, скрытый, только для чтения)
- длину файла (для каталога - 0)
- зарезервированное поле, которое не используется
- номер первого кластера в цепочке кластеров, отведенных файлу или каталогу; получив этот номер, операционная система, обращаясь к таблице FAT, узнает и все остальные номера кластеров файла.

Итак, пользователь запускает файл на выполнение. Операционная система ищет файл с нужным именем, просматривая описания файлов в текущем каталоге. Когда найден требуемый элемент в текущем каталоге, операционная система считывает номер первого кластера данного файла, а затем по таблице FAT определяет остальные номера кластеров. Данные из этих кластеров считываются в оперативную память, объединяясь в один непрерывный участок. Операционная система передает управление файлу, и программа начинает работать.

Для просмотра и редактирования корневого каталога ROOT можно также использовать **утилиту Disk Editor**.

Вопросы для подготовки

1. Роль FS.
2. Организация файлового сервера.
3. Файловые системы.
4. Дисковые квоты.
5. Права доступа.

Лабораторная работа №3 "Настройка корпоративной сети"

Основы работы в Cisco Packet Tracer. Понятие VLAN. Построение корпоративной сети в Cisco Packet Tracer.

Лабораторная работа №4 "Файловые системы"

Основы работы с файловыми системами. Модели разграничения прав доступа. На установленной ОС Windows Server установить роль FS. Выполнить форматирование диска по параметрам предложенным преподавателям. Назначить дисковые квоты. Настроить права доступа.

Тема 3. ACTIVE DIRECTORY

Системные администраторы используют технологию Active Directory в Windows Server для хранения и организации объектов в сети в иерархическую защищенную логическую структуру, например пользователей, компьютеров или других физических ресурсов.

Лес и домен составляют основу логической структуры. Домены могут быть структурированы в лесу, чтобы обеспечить независимость данных и сервисов (но не изоляцию) и оптимизацию репликации. Разделение логических и физических структур улучшает управляемость системы и снижает административные затраты, потому что на логическую структуру не влияют изменения в физическом устройстве. Логическая структура позволяет контролировать доступ к данным, т.е. вы можете использовать логическую структуру для контроля доступа к различным блокам данных.

Данные, хранящиеся в Active Directory, могут поступать из разных источников. С большим количеством различных источников данных и множеством различных типов данных Active Directory должен использовать некоторый стандартизованный механизм хранения, чтобы поддерживать целостность хранящейся информации.

В Active Directory объекты используют каталоги для хранения информации, все объекты определены в схеме. Определения объектов содержат информацию, такую как тип данных и синтаксис, которую каталог использует, чтобы гарантировать достоверность хранения. Никакие данные не могут быть сохранены в каталоге, пока они не определены в схеме. Схема по умолчанию содержит все определения и описания объектов, которые необходимы для корректной работы Active Directory.

Когда вы имеете доступ к каталогу через логическую структуру, состоящую из таких элементов, как домены и леса, сам каталог реализуется через физическую структуру, состоящую из базы данных, которая хранится на всех контроллерах домена в лесу.

Хранилище Active Directory обрабатывает весь доступ к БД. Хранилище данных состоит из служб и физических файлов, которые управляют правами доступа, процессами чтения и записи данных внутри базы данных на жестком диске каждого контроллера.

Структура и архитектура хранилища Active Directory

Структура и архитектура хранилища Active Directory состоит из четырех частей:

ДОМЕНЫ И ЛЕСА

Леса, домены и организационные единицы (OU) составляют основные элементы логической структуры Active Directory. Лес определяет единый каталог и представляет границу безопасности. Леса содержат домены.

DNS

DNS обеспечивает разрешение имен в иерархической архитектуре, которую может использовать Active Directory.

СХЕМА (SCHEMA)

Схема содержит определения объектов, которые используются для создания объектов, хранящихся в каталоге.

ХРАНИЛИЩЕ ДАННЫХ (DATA STORE)

Хранилище данных — это часть каталога, который управляет хранением и извлечением данных на каждом контроллере домена.

С помощью Active Directory можно поделить компьютеры на различные рабочие группы (организационные подразделения). Это существенно упрощает использование инфраструктуры в двух случаях:

Изменение существующих настроек группы. Поскольку настройки хранятся в единой базе данных, при их модификации, они будут применены для всех компьютеров, относящихся к этой группе.

Добавление нового пользователя. Он автоматически получает установленные для его группы настройки, что существенно ускоряет создание новой учетной записи.

В зависимости от пользователя (учетной записи, которая используется) и его группы можно ввести ограничение на использование функционала операционной системы.

Безопасность

Службы Active Directory существенно увеличивают защиту корпоративной сети. Так, все данные (учетные записи) хранятся на контроллерах доступа, которые защищены от внешнего доступа. Кроме того, для аутентификации в AD используется протокол Kerberos (протокол для взаимной аутентификации клиента и сервера перед установкой соединения, в нем учтена перехвата и модификации пакетов, что повышает его надежность), который значительно безопаснее аналога в рабочих группах.

Удобный обмен файлами

С помощью AD достаточно легко реализуется технология Distributed File System (DFS), которая используется для управления файлами. Фактически, это распределенная сеть для хранения файлов - физически они располагаются на нескольких серверах, но логически находятся в одном месте.

Это удобная функция, позволяющая масштабировать существующую инфраструктуру, добавляя новые сервера, а не заменяя ими старые.

Вопросы для подготовки

1. Роль AD.
2. Настройка контроллера домена.
3. Хозяин операций.
4. Групповые политики.

Лабораторная работа №5 "Основы работы с сетевыми хранилищами"

Принципы построения и организации центров обработки данных. Для центра обработки данных организовать сетевое хранилище под параметры, предложенные преподавателем

Лабораторная работа №6 "Основы работы с Active Directory"

Определение контроллера домена. Работа с групповыми политиками. На установленную ОС Windows Server установить роль AD. Выполнить основные настройки контроллера домена. Создать несколько пользователей. Создать и настроить групповые политики.

Тема 4. ВЕБ-БЕЗОПАСНОСТЬ

Есть пять основных элементов системы безопасности, предлагаемых IIS: проверка подлинности, управление доступом, шифрование, аудит и сертификаты

Проверка подлинности

IIS предлагает возможности обеспечения безопасности, полностью встроенные в Windows. Поддерживается пять методов проверки подлинности, поэтому можно подтвердить подлинность любого пользователя, запрашивающего доступ к веб-узлам.

Анонимная проверка подлинности позволяет получить доступ без указания имени пользователя и пароля.

Обычная проверка подлинности запросит имя пользователя и пароль, которые передаются по сети незашифрованными.

Краткая проверка подлинности является новой возможностью, которая выполняется так же, как и обычная, за исключением того, что пароли передаются в виде значения хэша. Значение хэша — это число, получаемое из текстового сообщения, например пароля. Исходный текст из значения хэша получить невозможно. Краткая проверка подлинности доступна только для доменов, контроллеры которых управляются операционной системой Windows 2000.

Встроенная проверка подлинности Windows использует технику хэширования для идентификации пользователя без фактической передачи пароля по сети.

Сертификаты представляют собой цифровое «удостоверение личности», которое может быть использовано для установления соединения по протоколу SSL. Они также могут быть использованы для проверки подлинности.

Эти методы могут быть использованы для разрешения доступа к общим областям узла и предотвращения несанкционированного доступа к личным файлам и каталогам.

Управление доступом

Основой системы безопасности веб-сервера являются разрешения на доступ файловой системы NTFS, позволяющие определить уровень доступа к файлам и каталогам, предоставляемого пользователям и группам Windows. Например, если фирма решает опубликовать на веб-сервере свой каталог, необходимо создать учетную запись пользователя Windows для этой организации, а затем сконфигурировать разрешения для конкретного веб-узла, каталога или файла. Эти разрешения должны допускать обновление содержимого веб-узла только администратором сервера и владельцем фирмы. Остальным пользователям следует разрешить просматривать веб-узел, но запретить изменение его содержимого.

WebDAV — это расширение протокола HTTP 1.1, которое облегчает работу с файлами и каталогами при соединении по протоколу HTTP. С помощью команд WebDAV можно добавлять и считывать свойства файлов и каталогов. Файлы и каталоги можно удаленно создавать, удалять, перемещать и копировать. Дополнительный контроль доступа можно настроить как через разрешения веб-сервера, так и через NTFS.

Сертификаты

Сертификаты представляют собой цифровые документы, удостоверяющие личность, которые позволяют и серверам, и клиентам проверить подлинность друг друга. Они необходимы для установления между сервером и обозревателем на компьютере клиента соединения по протоколу SSL, при котором информация может быть передана в зашифрованном виде. В IIS возможности SSL, основанные на использовании сертификатов, состоят из сертификата сервера, клиентского сертификата и различных цифровых ключей. Эти сертификаты могут быть созданы с помощью служб

сертификации Microsoft или получены от доверенной для обеих сторон независимой организации, называемой службой сертификации.

Шифрование

Можно разрешить пользователям обмениваться с сервером частными сведениями, например номерами кредитных карт или телефонами, безопасным путем с помощью шифрования. Шифрование «перемешивает» информацию перед ее пересылкой, дешифрование — расшифровывает ее после получения. Основанием для этого шифрования в IIS является протокол SSL 3.0, который обеспечивает безопасный способ установления зашифрованного соединения с пользователями. SSL подтверждает подлинность содержимого веб-узла и пользователей, пытающихся получить доступ к веб-узлам.

Сертификаты включают ключи, используемые при установке безопасного соединения по протоколу SSL. Ключ представляет собой уникальное значение, используемое для проверки подлинности сервера и клиента при установлении соединения SSL. Открытый ключ и закрытый ключ образуют пару ключей SSL. Веб-сервер использует пару ключей для установления безопасного соединения с веб-обозревателем клиента для определения уровня шифрования, необходимого для безопасной связи.

Для такого типа соединения необходимо, чтобы веб-сервер и веб-обозреватель пользователя были оснащены совместимыми системами шифрования и дешифрования. В процессе обмена создается ключ шифрования (или ключ сеанса). Ключ сеанса используется как сервером, так и веб-обозревателем для шифрования и дешифрования передаваемых данных. Степень шифрования для ключа сеанса, которую иногда называют стойкостью, измеряется в битах. Чем длиннее ключ сеанса, тем выше уровень шифрования и степень защиты. Хотя большая стойкость ключа обеспечивает большую безопасность, она также требует больше ресурсов сервера для реализации. Ключ сеанса веб-сервера обычно имеет длину 40 бит,

но может быть длиной до 128 бит, в зависимости от требуемого уровня безопасности

Аудит

Средства аудита дают широкие возможности контроля за посетителями и операциями веб-сервера. Рекомендуется регулярно выполнять аудит конфигурации сервера, чтобы обнаружить области, которые могут допустить несанкционированный доступ. Можно использовать встроенные служебные программы Windows, средства ведения журналов, встроенные в IIS 5.0, или использовать приложения ASP для создания собственного журнала аудита.

Реализованные стандарты

Большинство возможностей системы безопасности IIS реализуют стандарты, используемые в Интернете. Эти стандарты помогают поддерживать единообразие и использование приложений и информации на разных аппаратных платформах. Корпорация Майкрософт считает необходимым работать с пользователями компьютеров и Интернета, как помогая создавать хорошие стандарты, так и реализовывая эти стандарты. Для получения дополнительных сведений о стандартах, реализованных в IIS, следуйте соответствующей ссылке в приведенном ниже списке:

(SSL 3.0) — это основанный на открытых ключах протокол безопасности, реализованный Secure Channel (Schannel). Протокол безопасности SSL широко используется в обозревателях Интернета и серверах для проверки подлинности, целостности сообщения и обеспечения конфиденциальности.

Обычная проверка подлинности является частью спецификации HTTP 1.0. Пароль пересылается по сети в формате Base64. Большинство обозревателей поддерживают эту спецификацию.

Краткая проверка подлинности является новой возможностью IIS 5.0, совместимой с прокси-серверами. Идентифицирующая информация передается по сети в виде значения хэша.

PKCS #7 описывает формат зашифрованных данных, например цифровых подписей или цифровых конвертов, которые надежно хранят информацию, содержащуюся в них. И те, и другие включены в возможности сертификатов в IIS.

PKCS #10 описывает формат запросов на сертификат, которые направляются в службы сертификации.

Настройка системы безопасности

Прежде чем приступать к настройке средств защиты веб-сервера, следует определить уровень безопасности, необходимый для защиты веб-узлов и узлов FTP. Например, если планируется создание веб-узла, на котором некоторым пользователям будет разрешен доступ к секретной информации, такой как финансовые или медицинские архивы, необходимо установить надежную конфигурацию системы защиты. Эта конфигурация должна позволять надежно проверять подлинность заданных пользователей и предоставлять доступ только им.

Безопасность веб-сервера в значительной степени зависит от конфигурации системы безопасности Windows. Без правильной настройки средств безопасности Windows защитить веб-сервер невозможно.

Если это еще не сделано, выполните следующие действия:

- Настройте учетную запись администратора Windows.
- Создайте и организуйте учетные записи пользователей.
- Создайте и организуйте группы.
- Определите политику безопасности Windows.

В рамках задания конфигурации системы безопасности следует также отформатировать раздел жесткого диска под файловую систему NTFS. Разделы NTFS обеспечивают более полные возможности контроля за доступом к файлам и каталогам, а также более эффективное сохранение данных, чем разделы системы FAT. Для преобразования раздела жесткого

диска к системе NTFS можно использовать служебную программу Windows Convert. Дополнительные сведения содержатся в документации Windows.

После этого следует определить, какие файлы и каталоги должны быть общедоступными для посетителей веб- и FTP-узлов. Общедоступные материалы и материалы с ограниченным доступом следует сохранять в разных каталогах.

Вопросы для подготовки

1. Роль IIS.
2. Создание HTTP сайта.
3. Создание FTP сайта.
4. Основные настройки.
5. Публикация на сервере.

Лабораторная работа №7 "Администрирование корпоративной сети"

Инструменты анализа загрузки сети. Системы балансировки трафика. Построение корпоративной сети в Cisco Packet Tracer.

Лабораторная работа №8 "Создание и публикация веб-сайта"

Основы работы с протоколами HTTP и HTTPS. Анализ защищенности веб-приложений. На установленную ОС Windows Server установить роль IIS. Создать простой одностраничный сайт. Создать FTP сайта с не менее чем тремя виртуальными каталогами. Выполнить публикацию.

Тема 5. ПОЧТОВЫЙ СЕРВЕР

Электронная почта - важное средство обмена информацией в современном мире.

Обмен электронными почтовыми сообщениями основан на использовании клиент-серверной архитектуры, где почтовые серверы играют роль компьютеров, осуществляющих получение, хранение и доставку почты по запросам пользователей.

Основные задачи администратора почтового сервера:

- Установка и конфигурирование почтового сервера;
- Управление почтовыми отделениями;
- Управление доступом пользователей - создание, изменение, удаление почтовых ящиков;
- Резервное копирование и восстановление пользовательских данных;
- Обеспечение безопасности - конфиденциальности, целостности и доступности данных;

Сетевые протоколы

Используется несколько сетевых протоколов, используемых для процессов приема-передачи, а также управления почтовыми сообщениями:

- Smtp
- pop3
- imap

Типы почтовых серверов

Для централизованного управления почтовыми сообщениями используются специализированные компьютеры– почтовые серверы.

Почтовый сервер - специализированное программное обеспечение, выполняющее необходимые функции обслуживания почтовых клиентов, приема и передачи почтовых сообщений.

На сервере может быть запущены модули поддержки нескольких почтовых протоколов:

- протоколы принудительной доставки (передача почты инициируется отправителем);
- протоколы доставки по запросу (передача инициируется получателем сообщения).

Протоколы принудительной доставки почты

Почтовые серверы могут отправлять почту не только между пользователями одного компьютера, но и на другие компьютеры.

Для таких процессов используются ретрансляторы почты - система, принимающая почту от одного компьютера и посылающая на другой.

В качестве протокола принудительной доставки почтовых сообщений используется протокол SMTP (Simple Mail Transport Protocol).

Важная особенность при работе такого протокола - компьютер-получатель должен быть доступен.

Серверы доставки по запросу

Последнее звено в цепи доставки почты обычно составляют серверы доставки по запросу.

Наиболее популярные протоколы данного класса - POP (Post Office Protocol), IMAP (Internet Message Access Protocol).

Данные протоколы используются, когда конечным получателем является рабочая станция, на которой не запущен сервер принудительной доставки

Серверы принудительной доставки почты

Серверы принудительной доставки почты – важнейший компонент в системе обмена электронной почты.

Для UNIX систем примерами могут служит следующие популярные почтовые сервера:

- sendmail

- qmail
- exim
- postfix

Для Windows систем можно использовать специализированные серверы (такие как Exchange) или службу SMTP, входящую в состав IIS, службу pop3, входящую в состав Windows Server.

Сервис SMTP

При пересылке сообщения SMTP-сервер вначале устанавливает соединение с ближайшим узлом.

Если это соединение не установлено или по каким-либо причинам недоступно, SMTP- сервер отклоняет прием сообщения от клиента и уведомляет его об ошибке.

По умолчанию SMTP-сервер напрямую соединяется с сервером, на котором находится домен-получатель сообщения.

Служба SMTP

В состав IIS 6 входит служба простого протокола электронной почты (SMTP).

Средства администрирования IIS позволяют сконфигурировать SMTP-сервер для распространения служб обмена сообщениями на разнообразные платформы.

Параметры конфигурации

При работе с SMTP-сервером администратор должен контролировать следующие параметры:

- Аутентификацию клиентов на SMTP-сервере перед отправкой сообщения;
- Передачу сообщений клиента на SMTP-сервер;
- Отправку сообщений с SMTP-сервера;
- Маршрутизацию сообщений с SMTP-сервера;
- Настройки SMTP для заданного домена SMTP.

Управление службой SMTP

Для управления службой SMTP необходимо открыть оснастку консоли управления Windows - Диспетчер служб IIS. В списке доступных серверов имеется и указатель на службу SMTP.

При выборе закладки для виртуального SMTP- сервера откроется список доменов и текущих сеансов.

Создание и настройка виртуального сервера

Для выполнения отправки электронных сообщений через сервер под управлением Windows Server на нем должна быть запущена служба SMTP.

Если данная служба установлена и работает, для ее использования необходим виртуальным сервер SMTP.

По умолчанию такой сервер создается при установке службы SMTP.

При добавлении виртуального SMTP-сервера мастер создания выполняет базовую настройку виртуального SMTP-сервера.

Виртуальные SMTP-серверы не могут быть созданы из файлов конфигурации или посредством выполнения сценария.

Создание виртуального сервера

Мастер создания виртуального SMTP-сервера позволяет выполнить создание в несколько этапов.

Параметры, заданные при создании, впоследствии могут быть изменены, за исключением домашнего каталога:

- Этап 1. Указание имени виртуального сервера (используется для идентификации сервера в Диспетчере IIS).
- Этап 2. Задание IP-адреса виртуального SMTP-сервера (значение по умолчанию - все незанятые).
- Этап 3. Выбор домашнего каталога (домашним каталогом является путь к месту расположения в главном сервере, в который SMTP- служба записывает сообщения и файлы).

- Этап 4. Определение домена по умолчанию (домен по умолчанию - имя домена, присоединяемое к данному имени учетной записи в процессе аутентификации).

Структура домашнего каталога

В домашнем каталоге виртуального SMTP-сервера создаются следующие подкаталоги:

- BadMail. Каталог для записи сообщений, вернувшихся с отчетом о невозможности доставки.
- Drop. Каталог для записи всех входящих сообщений данного домена.
- Pickup. Каталог для записи сообщений, используемых службой сообщений.
- Queue. Каталог, в котором сообщения электронной почты ставятся в очередь для использования удаленно инициированной доставки при наличии поддержки удаленного домена.

Управление входящими сообщениями

Для виртуального SMTP- сервера можно также настроить параметры входящих сообщений:

- Ограничение на размер сообщения
- Ограничение на размер сеанса (суммарный объем всех сообщений за один сеанс)
- Ограничение числа сообщений за один сеанс
- Ограничение числа получателей одного сообщения
- Установка адреса для отправки отчетов о невозможности доставки
- Каталог для хранения ошибочной почты

Аутентификация входящих подключений

Параметры доступа к SMTP- серверу для клиентов задаются с помощью параметров во вкладке Доступ.

Возможны следующие варианты проверки подлинности:

- Анонимный доступ;
- Обычная проверка подлинности
- С использованием TLS- шифрования
- Встроенная проверка подлинности Windows

Ограничения по IP-адресам и именам доменов

Можно запретить или разрешить компьютерам с конкретным IP-адресом или именем домена доступ к виртуальному серверу SMTP.

Управление доступом осуществляется с помощью вкладки Доступ, дополнительное окно Подключение.

Вопросы для подготовки

1. Установка почтового сервера.
2. Основные настройки.
3. Организация в корпоративной сети.
4. Способы борьбы со спамом и нежелательной почтой.

Лабораторная работа №9 "Основы работы с лог-файлами"

Учет действий пользователей. Структура лог-файлов. Изучить лог-файлы с почтового сервера. Выполнить анализ трафика по критериям, предложенным преподавателем.

Лабораторная работа №10 "Анализ лог-файлов"

Алгоритмы и подходы анализа лог-файлов. Изучить лог-файлы с почтового сервера. Выполнить анализ трафика по критериям, предложенным преподавателем.

Тема 6. АНТИВИРУСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Антивирусное программное обеспечение создано для профилактики, выявления и уничтожения компьютерных вирусов. Способы обнаружения и лечения зараженных файлов могут быть разными. В любом случае при обнаружении заражения какого-либо файла антивирус пытается удалить из него вредоносный код и, если это сделать невозможно, удаляет файл полностью.

Типы антивирусного ПО

- Сканеры. После запуска сканируют файловую систему и ОЗУ (оперативную память) ПК и нейтрализуют найденные вирусы.
- Мониторы (сторожа). Отслеживают запускаемые на компьютере процессы в реальном времени.
- Полифаги. Наиболее эффективные, универсальные решения. Сканируют запускаемые файлы и загрузочные секторы жестких дисков на предмет появления новых вирусов.
- Блокировщики. Могут обнаружить компьютерный вирус на ранней стадии заражения ПК (при его записи в загрузочный сектор жесткого диска).
- Ревизоры. Создают базу сведений о параметрах файлов и контролируют их изменение. Не могут находить вирусы в новых файлах, так как не имеют о них данных в своей базе.

Блокировщики часто входят в BIOS (Basic Input-Output system – базовая система ввода/вывода, которая хранится на микросхеме материнской платы). Полифаги наиболее «тяжеловесные», они занимают много места на диске и «съедают» большой объем оперативной памяти.

Разновидности защит

В зависимости от типа угрозы (известная или неизвестная конкретному ПО) антивирус может осуществить проактивную или реактивную защиту:

Проактивная защита (эвристика). Защита от неизвестных вирусов, основанная на изучении кода и поведения программ, характерных для вредоносного ПО. Такой тип защиты показывает лучший результат при борьбе с модифицированными вирусами. За основу принимаются данные об существующих угрозах. Эвристика в антивирусном контексте — набор правил, которые используются для обнаружения действий вредоносных программ без необходимости определения конкретной угрозы.

Реактивная защита (вирусная сигнатура). Защита от уже известных вирусов, основанная на информации о коде и остальных особенностях вредоносного ПО. Для максимально эффективной работы такие антивирусы должны постоянно обновлять свои базы данных вирусных сигнатур. Защита, основанная на вирусных сигнатурах подразумевает обращение к словарю с уже известными вирусами, которые составили разработчики антивирусного ПО.

Главный недостаток проактивной защиты — так называемые «ложные срабатывания», частые блокировки незараженного программного обеспечения. Минус реактивной защиты — невозможность защититься от новых угроз. В современном антивирусном ПО используется и проактивная, и реактивная защита.

Как только антивирус обнаруживает вредоносный код, он может выполнить следующие действия (в зависимости от настроек пользователя):

Попытаться «вылечить» зараженный файл, убрав из него вредоносный код.

Отправить инфицированный файл в карантин. Актуально для ценных пользователю файлов. Находясь в карантине, зараженный файл не сможет навредить ПК; позже его можно вылечить самостоятельно или с помощью сторонних специалистов.

Удалить зараженный файл. Если исправить код не удалось, файл можно безвозвратно удалить с жесткого диска.

Не выполнять никаких действий. Если предполагается, что файл был помечен как «вредоносный» по ошибке, можно добавить этот файл в список исключений антивируса.

Полноценное антивирусное ПО защищает компьютер в режиме реального времени постоянно. То есть антивирус загружается вместе с ОС, всегда держит под контролем ОЗУ и файловую систему ПК, а также проводит мониторинг всех запускаемых и скачиваемых программ. Антивирусное программное обеспечение значительно снижает риск потери ценных данных, а также предотвращает попадание на ПК вредоносного ПО.

Вопросы для подготовки

1. Антивирусная защита.
2. Ядро антивируса.
3. Установка централизованной консоли управления антивирусом под ОС Windows Server.

Лабораторная работа №11 "Основы работы с антивирусным программным обеспечением"

Сигнатурный анализ. Принципы работы и настройки антивирусного программного обеспечения. На установленную ОС Windows Server установить централизованную консоль управления антивирусом KES. Установить ядро KES.

Лабораторная работа №12 "Настройка антивирусного программного продукта"

Создание задач и групповых политик в рамках антивирусного программного продукта. В централизованной консоли управления антивирусом KES выполнить необходимые настройки, создать задачи и групповые политики.

Тема 7. ЗАЩИТА БЕСПРОВОДНЫХ СЕТЕЙ

Различают несколько основных видов атак, которые угрожают безопасности беспроводных компьютерных сетей:

- «человек посередине»;
- DDoS-атаки;
- ложная точка доступа;
- атаки на сетевое оборудование.

Каждый из этих типов может применяться хакерами в определенных условиях с разными целями.

«Человек посередине»

«Человек посередине», или Man-in-the-Middle, относится числу наиболее распространенных типов атак. Этот способ чаще всего применяется для подключения к точкам доступа, не защищенным паролем. Поскольку сигнал в таких сетях транслируется без шифрования, злоумышленник может легко перехватывать его при помощи обычного ноутбука или компьютера с адаптером Wi-Fi. Однако возможно хакер может подключиться и к запаролированной сети при помощи специальной программы для взлома паролей методом подбора.

Атаки типа Man-in-the-Middle в свою очередь подразделяются на два вида — подслушивание и манипуляция.

«Подслушивание» называют еще **пассивной атакой**. Оно выполняется при помощи специального программного обеспечения, которое после получения доступа в локальную сеть отображает на компьютере злоумышленника весь трафик пользователя. Это может быть история посещения сайтов, вводимые логины и пароли, данные пластиковых карт и другая конфиденциальная информация.

Атаки типа «Манипуляция» называют **активными.** В этом случая хакер получает возможность не только кражи персональных данных пользователя, но и манипуляции его устройством через беспроводную сеть. Например, при

помощи специального ПО на компьютер пользователя может быть отправлена от имени точки доступа команда переадресации браузера на определенную страницу в интернете. На этой страницы компьютер заражается вирусами или другими вредоносным программным обеспечением.

DDoS-атаки

Еще одним распространенным типом угроз, которые необходимо учитывать в стандартах безопасности беспроводных сетей, являются DDoS-атаки, или отказ в обслуживании. Целью злоумышленников является нарушение работы локальной сети, при котором ее невозможно полноценно использовать. Атака может производиться на программном и на аппаратном уровне. В первом случае хакеры используют существующие уязвимости в программном обеспечении. Атака на аппаратном уровне выполняется за счет переполнения системы запросами, что приводит к исчерпанию ее ресурсов (дискового пространства, процессорного времени, пропускной способности и т. д.).

DDoS-атаки на программном уровне чаще всего выполняются за счет уязвимостей в протоколе. Они могут приводить к полной потере работоспособности подключенного к сети устройства. Например, может зависать компьютер, изменяются конфигурации операционной системы, или она получает повреждения.

При атаках на аппаратном уровне злоумышленник стремится добиться неработоспособности канала связи. Это достигается за счет направления массивных потоков бессмысленных данных, перегружающих канал, или созданием мощных помех. Помехи создаются при помощи специальных генераторов электромагнитного излучения.

Ложная точка доступа

Этот тип атак применяется злоумышленниками в местах, где действует общественная точка доступа, например, в кафе, в транспорте и т. д. Хакер через смартфон или ноутбук создает незапаролированную точку доступа, которая маскируется под легальную. Пользователи при попытке подключения

к общественному Wi-Fi, видят в списке доступных сетей ложную точку доступа и подключаются к ней. В результате злоумышленник перехватывает весь передаваемый трафик, включая конфиденциальные данные.

Часто нарушители, использующие ложные точки, могут подавлять сигнал легальной точки доступа при помощи специального оборудования. Это значительно увеличивает количество подключений жертв.

Атаки на сетевое оборудование

Точки доступа и другое сетевое оборудование с неправильно выстроенной конфигурацией и недостаточно эффективной защитой часто становится каналом для проникновения хакеров в локальную беспроводную сеть. Более того, беспроводные сети в итоге, как правило, коммутируются с проводными. Поэтому взлом сетевого оборудования создает угрозу безопасности и проводных сетей.

Обеспечить безопасность устройства беспроводного доступа и, соответственно, свести к минимуму связанный с этим видом доступа риск можно с помощью следующих несложных шагов.

Измените пароль администратора в своем беспроводном устройстве. Хакеру легко выяснить, какой пароль устанавливается по умолчанию производителем устройства, и использовать этот пароль для доступа в вашу беспроводную сеть. Избегайте паролей, которые легко подобрать или угадать (см. указания в разделе, посвященном выбору паролей).

Отключите трансляцию идентификатора сети (SSID broadcasting; SSID – Service Set Identifier, идентификатор сети), чтобы ваше беспроводное устройство не транслировало в эфир информацию о том, что оно включено.

Включите шифрование трафика: лучше всего использовать протокол WPA, если ваше устройство его поддерживает (если нет, используйте WEP-шифр).

Смените идентификатор сети (SSID) вашего устройства. Если оставить идентификатор, установленный по умолчанию производителем устройства, злоумышленник, узнав этот идентификатор, сможет легко "засечь" вашу

беспроводную сеть. Не используйте имена, которые легко угадать (см. указания в разделе, посвященном выбору паролей).

Вопросы для подготовки

1. Беспроводные сети.
2. Беспроводные маршрутизаторы.
3. Основные настройки и администрирование.

Лабораторная работа №13 "Основы работы с беспроводными технологиями"

Принципы построения и организации беспроводных сетей. Используя онлайн ресурсы, выполнить конфигурацию беспроводного маршрутизатора.

Лабораторная работа №14 "Основы построения беспроводных сетей"

Понятие зоны покрытия. Знакомство с сетевым оборудованием для организации беспроводных сетей. Используя онлайн ресурсы, выполнить расстановку беспроводных маршрутизаторов или антенн для полного покрытия зон здания беспроводной сетью. План здания в графическом файле предоставляет преподаватель.

Тема 8. ПРИНЦИПЫ РАБОТЫ МЕЖСЕТЕВЫХ ЭКРАНОВ

Межсетевые экраны (firewall, брандмауэр) делают возможной фильтрацию входящего и исходящего трафика, идущего через вашу систему. Межсетевой экран использует один или более наборов правил для проверки сетевых пакетов при их входе или выходе через сетевое соединение, он или позволяет прохождение трафика или блокирует его. Правила межсетевого экрана могут проверять одну или более характеристик пакетов, включая, но не ограничиваясь типом протокола, адресом хоста источника или назначения и портом источника или назначения.

Межсетевой экран располагается между защищаемой (внутренней) сетью и внешней средой (внешними сетями или другими сегментами корпоративной сети). В первом случае говорят о внешнем МЭ, во втором – о внутреннем. Межсетевой экран – идеальное место для встраивания средств активного аудита. МЭ способен реализовать сколь угодно мощную реакцию на подозрительную активность, вплоть до разрыва связи с внешней средой.

На межсетевой экран целесообразно возложить идентификацию/аутентификацию внешних пользователей, нуждающихся в доступе к корпоративным ресурсам (с поддержкой концепции единого входа в сеть).

Межсетевые экраны могут серьезно повысить уровень безопасности хоста или сети. Они могут быть использованы для выполнения одной или более нижеперечисленных задач:

- Для защиты и изоляции приложений, сервисов и машин во внутренней сети от нежелательного трафика, приходящего из внешней сети интернет.
- Для ограничения или запрещения доступа хостов внутренней сети к сервисам внешней сети интернет.
- Для поддержки преобразования сетевых адресов (network address translation, NAT), что дает возможность задействовать во внутренней

сети приватные IP адреса и совместно использовать одно подключение к сети Интернет (либо через один выделенный IP адрес, либо через адрес из пула автоматически присваиваемых публичных адресов).

Существует два основных способа создания наборов правил межсетевого экрана: **включающий и исключающий.**

Исключающий межсетевой экран позволяет прохождение всего трафика, за исключением трафика, соответствующего набору правил. Включающий межсетевой экран действует прямо противоположным образом. Он пропускает только трафик, соответствующий правилам, и блокирует все остальное.

Включающий межсетевой экран обеспечивает гораздо большую степень контроля исходящего трафика. Поэтому включающий межсетевой экран является лучшим выбором для систем, предоставляющих сервисы в сети Интернет. Он также контролирует тип трафика, порождаемого вне и направляющегося в вашу приватную сеть. Трафик, не попавший в правила, блокируется, а в файл протокола вносятся соответствующие записи. Включающие межсетевые экраны обычно более безопасны, чем исключающие, поскольку они существенно уменьшают риск пропуска межсетевым экраном нежелательного трафика.

Безопасность может быть дополнительно повышена с использованием межсетевого экрана с сохранением состояния. Такой межсетевой экран сохраняет информацию об открытых соединениях и разрешает только трафик через открытые соединения или открытие новых соединений.

Недостаток межсетевого экрана с сохранением состояния в том, что он может быть уязвим для атак DoS (Denial of Service, отказ в обслуживании), если множество новых соединений открывается очень быстро. Большинство межсетевых экранов позволяют комбинировать поведение с сохранением

состояния и без сохранения состояния, что позволяет создавать оптимальную конфигурацию для каждой конкретной системы.

Вопросы для подготовки

1. Основные положения по работе межсетевых экранов.
2. Основной функционал.
3. Настройки.

Лабораторная работа №15 "Основы работы с межсетевыми экранами"

Обзор межсетевых экранов и знакомство с принципами их работы. Моделирование сетевых правил на межсетевых экранах при помощи современных онлайн сервисов.

Лабораторная работа №16 " Настройка межсетевых экранов"

Основы написания сетевых правил фильтрации трафика. Моделирование сетевых правил на межсетевых экранах при помощи современных онлайн сервисов.

Тема 9. СЕТЕВЫЕ АТАКИ

Сетевой атакой называю намеренные действия третьих лиц, направленные на установлению контроля над локальным или удаленным компьютером или вычислительной системой. В результате атак злоумышленники могут нарушать работу сети, изменять права аккаунта, получать персональные данные пользователей и реализовывать другие цели.

Виды сетевых атак и их последствия имеют значительные отличия друг от друга. Современная классификация угроз проводится по следующим параметрам:

- характер воздействия, оказываемого на сеть;
- цель оказываемого воздействия;
- наличие обратной связи с сетью, подвергнутой атаке;
- условие начала атаки;
- расположение субъекта по отношению к объекту атаки;
- уровень эталонной модели ISO.

По характеру воздействия на сеть

Виды сетевых атак по характеру воздействия на атакуемую сеть можно разделить на **активные и пассивные.**

Активная атака проводится с непосредственным воздействием на сеть, которые может предусматривать ограничение ее работоспособности, модификацию настроек. Воздействие такого рода обязательно оставляет следы, поэтому при его планировании изначально предусматривается обнаружение.

Пассивная атака проводится без непосредственного влияния на работу сети. Однако в ее результате нарушается сетевая безопасность. Обнаружить пассивную атаку намного сложнее именно из-за отсутствия прямого воздействия. Примером таких угроз можно назвать постановку наблюдения или прослушки.

По цели атаки

В зависимости от цели различают виды сетевых атак, направленных на нарушение:

- функционирования;
- конфиденциальности;
- целостности атакуемой сети.

Основной целью является, как правило, несанкционированный доступ к закрытой информации методом ее искажения или перехвата. В первом случае сведения могут быть изменены, во втором – доступ производится без изменения данных.

По наличию обратной связи с атакуемой сетью

Атака может проводиться с обратной связью или без нее (однонаправленная атака).

В первом случае атакующим субъектом устанавливается обмен данными с атакуемым объектом. В результате злоумышленники получают актуальные данные о состоянии сети.

Однонаправленная атака не предусматривает установления обратной связи. Ее проводят, когда для реализации целей злоумышленников не требуется оперативной реакции на изменения состояния объекта.

По условию начала атаки

Существуют разные условия начала воздействия. В том числе можно выделить такие типы сетевых атак по этому критерию:

- по запросу от объекта;
- по выполнению на стороне объекта определенного действия;
- безусловные атаки.

Первые два типа атак начинаются после соответствующего события, а безусловные – в любой момент.

По расположению субъекта по отношению к объекту атаки

По этому критерию различают сетевые атаки межсегментного и внутрисегментного типа. Особенностью категории первого типа является расположение субъекта и объекта в разных сегментах сети. Второй тип характеризуется их расположением в одном сегменте.

Сегментом сети называю хосты (компьютеры), физически объединенные между собой.

По уровню эталонной модели ISO/OSI

Воздействие на атакуемую сеть может осуществляться на разных уровнях эталонной модели ISO/OSI.

В том числе выделяются такие уровни:

- физический;
- сетевой;
- транспортный;
- канальный;
- сеансовый;
- прикладной;
- представительный.

Примеры атак

В качестве примеров наиболее распространенных сетевых атак можно привести следующие виды воздействия:

Применение нестандартных протоколов. Тип протокола пакета данных определяется по содержащемуся в нем специальному полю. При изменении злоумышленниками значения в этом поле осуществляется передача данных, которую система не может определить.

Ping Flooding. Такая атака может быть реализована только при условии доступа к высокоскоростному интернету. Она предусматривает применение флудинга вместо стандартной команды контроля пинга. В результате создается избыточная нагрузка на сеть, что приводит к нарушениям в ее работе.

Фрагментация данных. При передаче по IP пакет данных делится на части, а на стороне получателя – собирается. В случае атаки выполняется отправка значительного числа подобных фрагментов с засорением буфера обмена и нарушениям работы сети.

Технологии обнаружения атак и алгоритмы действий по их устранению

В связи с быстрым развитием информационных технологий и технических средств статичные механизмы защиты от сетевых угроз часто оказываются неэффективными. Обеспечить эффективную защиту информации позволяют динамические методы, способные оперативно выявлять и устранять угрозы. Работа динамических технологий строится на оценки уровня подозрительности действий в сети со стороны определенной службы или процесса.

Алгоритм действия по устранению атак направлен на идентификацию подозрительных объектов. После этого система реагирует необходимым образом на деятельность таких объектов, которая может быть нацелена на ресурсы сети или компьютерного оборудования.

Методы защиты

Для защиты сетей от внешних угроз могут применяться следующие основные методы и технологии:

- применение портов высокой надежности, шифрование данных;
- использование эффективных антивирусов и сканеров;
- применение программного или аппаратного сетевого экрана;
- установка блокираторов руткитов и снифферов.

Вопросы для подготовки

1. Межсетевые экраны.
2. Процесс формирования адресной книги и сетевых правил.
3. Способы борьбы с атаками.
4. Лицензии.

Лабораторная работа №17 "Работа с сетевыми правилами межсетевых экранов"

Основы анализа и поиска вредоносного трафика. Написание сетевых правил межсетевого экрана корпоративной сети.

Лабораторная работа №18 "Реализация основных моделей доступа средствами межсетевых экранов"

Разграничение прав доступа с помощью межсетевых экранов. Написание сетевых правил межсетевого экрана корпоративной сети.

СПИСОК ЛИТЕРАТУРЫ

1. **Богданова, С.В. Информационные технологии [Электронный ресурс]**: учебное пособие / С. В. Богданова, А. Н. Ермакова. - Ставрополь: Сервисшкола, 2014. - 211 с. - Режим доступа: http://znanium.com/catalog.php?bookinfo=514867/ (дата обращения: 15.05.2020).
2. **Партыка Т. Л. Информационная безопасность [Электронный ресурс]:** Учебное пособие / Т.Л. Партыка, И. И. Попов. - 5-е изд., перераб, и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с. - Режим доступа: http://znanium.com/catalog/product/420047/ (дата обращения: 15.05.2020).
3. **Гагарина, Л. Г. Информационные технологии [Электронный ресурс]:** учебное пособие / Л. Г. Гагарина, Я. О. Теплова, Е. Л. Румянцева и др.; под ред. Л. Г. Гагариной - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2015. - 320 с. - Режим доступа: http://znanium.com/catalog/product/471464/ (дата обращения: 15.05.2020).

Интернет-ресурсы

1. Документы IETF – инженерного совета Интернета. - http://www.ietf.org/rfc.html [On-line] (дата обращения: 15.05.2020).