Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Ганеев Винер Валиахметович
Должность: Директор
Дата подписания: 13.11.2026 15:50:25
Уникальный программный ключ:
fceab25d7092f3bff743e8ad3f8d57fddc1f5e66

Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «Уфимский университет науки и технологий»

Бирский филиал

ФАКУЛЬТЕТ ФИЗИКИ И МАТЕМАТИКИ

УТВЕРЖДАЮ:
Декан
подписано ЭЦП Гайсин Ф.Р.
(подпись, инициалы, фамилия)

«26» 02 2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность
(наименование дисциплины)

ОПОП ВО программа бакалавриата
09.03.03 Прикладная информатика
шифр и наименование направления подготовки (специальности)

направленность (профиль, специализация)

Прикладная информатика в информационной сфере
наименование направленности (профиля, специализации)

форма обучения
очная
(очная, очно-заочная, заочная)

Бирск 2026 г.

Рабочая программа составлена на основании учебного плана основной профессиональной образовательной программы 09.03.03 Прикладная информатика профиль Прикладная информатика в информационной сфере, одобренного ученым советом Бирского филиала Уфимского университета науки и технологий (протокол №7 от 27.02.2026 г.) и утвержденного директором Бирского филиала 27.02.2026.

Зав.кафедрой кафедры информатики и экономики *(наименование кафедры разработчика программы)*	*подписано ЭЦП*	Стовба Е.В.
Разработчик программы	*подписано ЭЦП*	Дударева О.В.
Руководитель образовательной программы	*подписано ЭЦП*	Бигаева Л.А.

1. Цель дисциплины. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

1.1. Цель дисциплины

Цель изучения дисциплины: формирование знаний о видах угроз информационной безопасности и её стандартах, методах и средствах борьбы с угрозами информационной безопасности, представлений о политике безопасности и её типах, умений и навыков решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Выработка способности участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью,определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

Таблица 1. – Результаты обучения по дисциплине

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной
код компетенции	наименование компетенции	
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1. Демонстрирует знания принципов, методов и средств решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности.
		ОПК-3.2. Демонстрирует навыки решения стандартных задач профессиональной деятельности и выбирает способы их решения с применением ИКТ, информационно-библиографических средств и с учетом требований информационной безопасности
		ОПК-3.3. Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
ОПК-4	Способен участвовать в разработке стандартов,	ОПК-4.1. Демонстрирует знания стандартов оформления технической документации на различных стадиях

	норм и правил, а также технической документации, связанной с профессиональной деятельностью	жизненного цикла информационной системы.
		ОПК-4.2. Участвует в разработке технической документации, связанной с профессиональной деятельностью.
		ОПК-4.3. Участвует в разработке стандартов, норм и правил оформления технической документации.
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1. Формулирует в рамках поставленной цели проекта совокупность взаимосвязанных задач, обеспечивающих ее достижение. Определяет ожидаемые результаты решения выделенных задач
		УК-2.2. Проектирует решение конкретной задачи проекта, выбирая оптимальный способ ее решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений
		УК-2.3. Решает конкретные задачи проекта заявленного качества и за установленное время

2. Структура и трудоемкость дисциплины

Общая трудоемкость (объем) дисциплины составляет 4 зачетные единицы (з.е.), 144 академических часов.

Таблица 2 – Объем дисциплины

Виды учебной работы	Всего, часов	Количество часов в семестре
Общая трудоемкость дисциплины	144	4 семестр - 144
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	56	4 семестр - 56
в том числе:		
лекции	24	4 семестр - 24
лабораторные занятия	22	4 семестр - 22
практические занятия	10	4 семестр - 10
Другие виды работ в соответствии с УП:		
контрольная работа	0	
консультации	0	
Самостоятельная работа обучающихся (всего)	88	4 семестр - 88
Из них:		
контроль	0	
ФКР:		
зачет	0.2	4 семестр - 1
зачет с оценкой	0	
курсовая работа (проект)	0	
экзамен	0	

3 Содержание дисциплины

Таблица 3 – Содержание дисциплины

№	Раздел (тема) дисциплины	Виды деятельности	Форма текущего

п/п		Лек, час.	Лаб, час.	П, час.	Зч, час.	СРС, час.	контроля успеваемости
2 курс / 4 семестр							
1	Раздел 1. Информационные ресурсы. Информационная безопасность.						
1.1	Информационные ресурсы Основные понятия, классификация информационных ресурсов	6	4	2		22	Тестирование, Групповой опрос, Лабораторная работа, Практические работы
1.2	Информационная безопасность Понятие информационной безопасности, классификация.Основные составляющие информационной безопасности. Классификация методов обеспечения информационной безопасности	6	6	2		22	Практические работы, Тестирование, Групповой опрос, Лабораторная работа
2	Раздел 2. Методы и средства защиты информации. Компьютерная безопасность.						
2.1	Методы и средства защиты информации. Правовая защита. Организационная защита. Инженерно-техническая защита. Криптографические средства защиты	6	6	2		21.8	Практические работы, Тестирование, Групповой опрос, Лабораторная работа
2.2	Компьютерная безопасность. Защита компьютерной информации от несанкционированного доступа. Угрозы безопасности информации в компьютерных системах. Парольная защита операционных систем	6	6	4		22	Лабораторная работа, Тестирование, Практические работы, Групповой опрос
3	Зачет				1	0.2	
Итого по 2 курсу 4 семестру		24	22	10	1	88	
Итого по дисциплине		24	22	10	1	88	

Таблица 4 – Лабораторные работы

№	Наименование лабораторных работ	Объем, час.

п/п		
2 курс / 4 семестр		
1.	Информационные ресурсы	4
2.	Информационная безопасность	6
3.	Методы и средства защиты информации	6
4.	Компьютерная безопасность	6

Таблица 5 – Практические (семинарские) занятия

№ п/п	Наименование семинарских и практических работ	Объем, час.
2 курс / 4 семестр		
1.	Информационные ресурсы	2
2.	Информационная безопасность	2
3.	Методы и средства защиты информации	2
4.	Компьютерная безопасность	4

4. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Критериями оценивания являются баллы, которые выставляются за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины. Баллы, выставляемые за конкретные виды деятельности представлены ниже.

Контрольные задания для проведения текущего контроля успеваемости

Тестовые задания

Описание тестовых заданий: тестовые задания включают тесты закрытого типа (с одним правильным ответом), тесты на установлении последовательности и на установление соответствия. Оценка за выполнение тестовых заданий выставляется на основании процента заданий, выполненных студентами в процессе прохождения промежуточного и рубежного контроля знаний

S: Информация это:
-:сведения, поступающие от СМИ
-:только документированные сведения о лицах, предметах, фактах, событиях
+:сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления
-:только сведения, содержащиеся в электронных базах данных

S: Информация
-:не исчезает при потреблении
-:становится доступной, если она содержится на материальном носителе
-:подвергается только "моральному износу"
+:характеризуется всеми перечисленными свойствами

S: Информация, зафиксированная на материальном носителе, с реквизитами, позволяющими ее идентифицировать, называется
-:достоверной
-:конфиденциальной
+: документированной
-:коммерческой тайной

S: Формы защиты интеллектуальной собственности -
+: авторское, патентное право и коммерческая тайна
-: интеллектуальное право и смежные права
-: коммерческая и государственная тайна
-: гражданское и административное право

S: По принадлежности информационные ресурсы подразделяются на
+: государственные, коммерческие и личные
-: государственные, не государственные и информацию о гражданах
-: информацию юридических и физических лиц
-: официальные, гражданские и коммерческие

S: К негосударственным относятся информационные ресурсы
-: созданные, приобретенные за счет негосударственных учреждений и организаций

-: созданные, приобретенные за счет негосударственных предприятий и физических лиц
-: полученные в результате дарения юридическими или физическими лицами
+: все указанные

S: По доступности информация классифицируется на
-: открытую информацию и государственную тайну
-: конфиденциальную информацию и информацию свободного доступа
+: информацию с ограниченным доступом и общедоступную информацию
-: виды информации, указанные в остальных пунктах

S: К конфиденциальной информации относятся документы, содержащие
+: государственную тайну
-: законодательные акты
-: "ноу-хау"
-: сведения о золотом запасе страны

S: Запрещено относить к информации ограниченного доступа
-: информацию о чрезвычайных ситуациях
-: информацию о деятельности органов государственной власти
-: документы открытых архивов и библиотек
+: все, перечисленное в остальных пунктах

S: К конфиденциальной информации не относится
-: коммерческая тайна
-: персональные данные о гражданах
-: государственная тайна
+: "ноу-хау"

Методические материалы, определяющие процедуру оценивания выполнения тестовых заданий

Описание методики оценивания выполнения тестовых заданий: оценка за выполнение тестовых заданий ставится на основании подсчета процента правильно выполненных тестовых заданий.
Критерии оценки (в баллах)*:*
- **9-10** баллов выставляется студенту, если процент правильно выполненных тестовых заданий составляет 81 – 100 %;
- **7-8** баллов выставляется студенту, если процент правильно выполненных тестовых заданий составляет 61 – 80 %;
- **4-6** баллов выставляется студенту, если процент правильно выполненных тестовых заданий составляет 41 – 60 %;
- **до 4** баллов выставляется студенту, если процент правильно выполненных тестовых заданий составляет 40 %;

Конспект

Примеры тем для конспектов:
Достоинства и недостатки реализации и обработки радиотехнических сигналов цифровыми методами.
Кодирование информации
«Несанкционированный» и «неавторизованный «доступ к информации».
Разница между “защитой информации” и “информационной безопасностью”
Блокировка неавторизованного доступа к информации.
Правовые аспекты защиты информации

Методические материалы, определяющие процедуру оценивания конспекта

Критерии оценки:
- оптимальный объем текста (не более одной трети оригинала);
- логическое построение и связность текста;
- полнота/ глубина изложения материала (наличие ключевых положений, мыслей);
- визуализация информации как результат ее обработки (таблицы, схемы, рисунки);
- оформление (аккуратность, соблюдение структуры оригинала).

1- выставляется, если текст конспекта оформлен аккуратно, выбрано главное и второстепенное, выделены ключевые слова и понятия, конспект написан лаконично с применением системы условных сокращений.

Практические работы

Практические работы, являются важным источником познания нового материала, способствуют формированию и совершенствованию практических умений и навыков обучающихся.
Практическая работа № 5 - 6

Организация функционирования ЛВС на базе операционной системы Windows 2003 Server. Установка ОС и построение контроллера домена.

Целью данной работы является приобретение навыков установки операционной системы (ОС) Windows 2003 Server и настройка сетевых служб ADS (Active Directory Services), DNS (Domain Name Server), DHCP (Dynamic Host Configuration Protocol). Построение Контроллера Домена (Domain Controller).

**Данное описание создано на базе VMWare Workstantion версии 5.0, поэтому размещение некоторых пунктов и очередность их следования может отличаться от программного обеспечения, установленного в учебных классах.*

Ход работы:

- Создание виртуальной машины

Запустите VMWare Workstantion. И выберите «New Virtual Machine»

Следуйте следующим экранам. Нажимаем «Далее».
Конфигурацию виртуальной машины уточните у преподавателя.

Выбираем тип и версию операционной системы. В нашем случае «Microsoft Windows» и «Windows 2003 Server Standard Edition».
Далее вводим наименование и размещение виртуальной машины.

Выбираем тип сетевого соединения для виртуальной машины.

Существует три основных режима подключения виртуальной машины к сети: Bridged mode, NAT и Host Only.
Bridged mode дает виртуальной машине непосредственный доступ к внешнему интерфейсу хост-машины, на котором виртуальная машина самостоятельно устанавливает или получает через

DHCP собственные сетевые параметры - такие как IP-адрес, маршрутизатор по умолчанию и тому подобные.
NAT использует трансляцию адресов исходящего трафика. Напомню, что в этом случае адрес виртуальной машины, полученный по встроенному в NAT DHCP, в момент пересылки на внешний протокол подменяется на адрес хост-машины.
Третий режим **Host Only** представляет дела так, будто у хост-машины в дополнение к имеющимся сетевым интерфейсам есть еще одна сетевая карточка (видимая в системе и без запуска VM), к которой подключается наша ВМ, образуя с хост-машиной маленькую подсеть. Таким образом, можно устроить сеть на одном компьютере.

Выбираем расположение образов операционной системы.
Для запуска виртуальной машины нажмите следующий значок

- Установка операционной системы

Windows Server 2003 *(кодовое название при разработке — Whistler Server, внутренняя версия — Windows NT 5.2) — это операционная система семейства Windows NT от компании Microsoft, предназначенная для работы на серверах. Она была выпущена 24 апреля 2003 года.* ***Windows Server 2003*** *является развитием Windows 2000 Server и серверной частью для операционной системы Windows XP.*

Перед нами стоит задача построить сеть из нескольких компьютеров и сделать один из них сервером. Начнем с установки. Мы будем устанавливать Windows Server 2003 Standard Edition. Установка с автозагружающегося CD-диска ничем не отличается от установки Windows 2000/XP. Во время настроек языка (Regional and Language Options) нажмите Customize и в закладке Regional Options, в пункте Standarts and formats выберите Ukraine (рис. 1). То же самое выберите в пункте Location в той же закладке. Далее нажмите закладку Advanced в поле Select a language to match the language version of the non-Unicode programs you want to use и выберите Russian. Тем самым мы обеспечили корректное отображение русского языка в программах, например Far или Total Commander, а также нормальное написание валюты, дат и чисел. Переходим к следующему пункту.

рис. 1

Введя имя и название организации, а также регистрационный ключ, попадаем в Режим лицензирования (Licensing Modes), где вам предложат два варианта: на сервер (Per Server) или же на устройство или пользователя (Per device or Per User) (рис. 2).

рис. 2

Для настройки сети мы выбираем настройки вручную. Выбираем ***Internet Protocol (TCP/IP)***, кликаем на кнопку ***Properties (Свойства)***, отменяем автоматическое получение IP-адреса, вбиваем 192.168.0.1 в поле ***IP address***, нажимаем *Tab*, — маска подсети должна автоматически заполниться и принять вид 255.255.255.0 (все остальные поля должны остаться пустыми). Нажав на *Далее*, мы увидим предложение подключить сервер либо к рабочей группе, либо к домену. Ни то, ни другое нам не надо, нажимаем кнопку *Далее* и ждем завершения установки (рис. 3).

рис. 3

Краткие теоретические сведенья:
*Что такое **маска подсети?** Это число, состоящее из четырех октетов, которые определят, какая часть IP-адреса является сетевым адресом, а какая — адресом хоста. Маска это делает, «маскируя» с помощью двоичного числа часть сетевого IP-адреса, отведенную для нумерации подсетей. Например, IP-адрес 207.29.170.193, а маска — 255.255.255.0. Тогда IP-адрес и маска в двоичном виде будут, соответственно, 11001111.11011011.10101010.11000001 и 11111111.11111111.11111111.00000000. Таким образом, все числа, «накрытые» маской, являются номерами подсетей, а последнее десятичное число, или же 8 бит, оставлено для адресов хостов подсети. При организации связей между компьютерами в сети как раз маски и используются для определения того, находится ли целевой хост в той же подсети, что и исходный. Если же он удаленный, т.е. не принадлежит этой подсети, исходный хост пошлет информацию по IP-адресу основного шлюза, который, как вы помните, в сетевой настройке сервера мы оставили пустым. Для определения местоположения целевого хоста компьютер применяет операцию ANDing для IP-адресов и масок обоих хостов. Операция ANDing работает следующим образом: взяв в двоичном виде IP-адрес и маску, сервер сравнивает их, и если в соответствующем разряде адреса и маски стоит 1, то результат будет 1. В противном случае результат — 0. Если результаты ее выполнения равны — оба компьютера находятся в одной подсети.*
***Domain Name Server** (сервер доменных имен) — сервер, содержащий базу данных с именами хостов и сопоставленными им IP-адресами. Таким образом, пользователи сети работают с именами хостов, а DNS уже преобразует их в настоящие IP-адреса. Почему мы его оставили пустым? Потому что сервер как раз и будет выполнять функции DNS. Ну вот, установка подходит к концу, перейдем к настройке сервера.*

- Назначение ролей нашему серверу

Для упрощения дальнейшей нашей работы воспользуемся возможностью ОС **Windows 2003 Server** по администрированию сервера, нажимаем *Пуск* (Start) > Управление Вашим Сервером (*Manage Your Server)*.

Нажимаем «Новая роль» (**New role)**, выбираем «Особая конфигурация» (**Custom configuration**)

Из списка доступных ролей выбираем «Контроллер домена» **Domain Controller (Active Directory)**

Далее выбираем Контроллер домена в новом домене **(Domain controller for new domain)**. Далее опции: «Новый домен в новом лесу» (**Domain in new forest)**

- Полное DNS-имя нового домена **(Full DNS name)** — mydomaine.com;

- **NetBIOS name** — MYDOMAINE;
- Следующие две страницы оставляем без изменений;

- Выбираем «Разрешения, совместимые только с Windows 2000 или Windows Server 2003» **(Permissions compatible with Windows 2000 or Windows Server 2003 operation systems)**

- вводим пароль администратора, перезагружаемся.

Как вы уже поняли, этой последовательностью действий мы сделали наш сервер Контроллером Домена (Domain Controller), а соответственно, «подняли» на нем службу Active Directory и, наконец, настроили DNS на нашем компьютере.

*Что такое **активный каталог**? Сети Windows 2000/XP/2003 структурируются с помощью служб активного каталога или **ADS** (Active Directory Services). Они устанавливаются и управляются средствами серверов Windows 2000/2003. Все компоненты компьютерной сети (т.е. компьютеры-пользователи, всевозможные сетевые ресурсы и т.д.) для ADS являются объектами, свойства которых определяются с помощью различных атрибутов. Все объекты, входящие в ADS, образуют каталог. Для удобства управления этими объектами в ADS используются контейнеры, задача которых состоит в хранении остальных объектов, а также в настройке их работы.*
Компьютеры могут объединяться в логические единицы, называемые доменами. Каждый домен управляется контроллером домена, хранящим общую для домена информацию и выполняющим общую централизованную авторизацию подсоединившихся пользователей. В отличие от доменов на базе Windows NT, контроллеров в доменах Windows 2000/2003 может быть несколько, и они равноправны. Для еще большего структурирования домены могут объединяться в «деревья».

Ну что ж, мы настроили DNS и ADS. Для легкости в расширении сети, ведь сейчас для того чтобы добавить компьютер в наш домен, нам необходимо выделить вручную ему IP-адрес и каждый раз прописывать маску, основной шлюз, предпочтительный и альтернативный адреса DNS. Хорошо, если у Вас несколько компьютеров, а если их сотни? И тут на арену выходит **DHCP** (Dynamic Host Configuration Protocol — протокол динамической конфигурации хоста), который, судя по названию, решит все эти проблемы. Давайте его установим и настроим.
В окне *Manage Your Server* нажимаем «Новая роль» (**New role) > DHCP Server**,
в окне **Имя области** вводим: *Name:* local.

*На следующей странице Start IP-Address:*192.168.0.1; *End IP-Address:* 192.168.0.100; маска подсети должна принять значение 255.255.255.0,

Исключения (Exclusions) пропускаем (если хотите, можете указать диапазон тех адресов, области из которых выбирать нельзя)
Длительность: 31 день (период резервирования адреса).
Далее выбираем *«Да, я хочу настроить эти опции сейчас»*, *Router* (Default Gateway) — 192.168.0.1 (Add), *Domain Name and DNS servers* — 192.168.0.1 (Add).
WINS Server я оставляю пустым, т.к. сеть у нас на основе Windows 2000/XP/2003 (этот сервер выполняет функции DNS для Windows 95/98/Me), *Yes, I want to activate this scope now* (Finish).

Далее, все в том же окне «Управление Вашим сервером» (**Manage Your Server**) выбираем пункт «Управление DHCP сервером» (**Manage this DHCP server)**, откроется окно, именуемое консолью для управления нашего DHCP-сервера. В левой части этого окна выбираем пункт такого вида: имя сервера.название домена [IP–адрес сервера] (в нашем случае: server.mydomaine.com [192.168.0.1]). Теперь в главном меню нажимаем пункт Действия > Авторизировать (**Action > Authorize)**, и таким образом мы авторизировали наш DHCP-сервер в сети.

- Настройка сетевого взаимодействия в VMWare

Для проверки правильности настройки нашего сервера необходимо организовать сетевое взаимодействие сервера с клиентами. В качестве клиента возьмем предварительно установленный образ «Windows XP».
Выполним следующие действия:

1. Завершим работу с серверной и клиентской ОС. Выполним команду «Отключить питание» (Power Off).
2. Создадим новую команду (Team). Выполним File>New>Team.
3. Добавим наши операционные системы (Server 2003 и XP) в команду.
4. Настроим сетевые параметры

- Добавление клиентских машин в домен

На клиентском компьютере выбираем *Пуск > Настройка > Сеть и удаленный доступ к сети*, кликаем правой кнопкой мыши на *Подключение по локальной сети*, выбираем *Свойства*, затем *Протокол Интернета (TCP/IP)*, опять же *Свойства*. Выбираем *Получить IP-адрес автоматически.*

Далее, нажав правой кнопкой мыши по иконке «Мой компьютер», выбираем *Свойства > Имя компьютера > Изменить*. В пункте «*Является членом* выбираем *домена»* и вводим выбранное имя домена (MYDOMAINE) и нажимаем OK. Выведется окно с запросом имени и пароля пользователя, который имеет соответствующие права для подключения компьютера в домен.

Вывод. Установив Windows 2003 Server и настроив некоторые службы, Вы познакомились с огромным миром серверных технологий. Это было лишь поверхностное ознакомление, на следующих занятиях мы изучим более детально возможности данной ОС.

Контрольные вопросы:

1. Что такое контроллер домена?
2. Для чего предназначена служба DNS?
3. Почему у сервера DNS должен быть статический IP- адрес?
4. Для чего предназначен протокол DHCP?
5. Назовите необходимые действия и их порядок для добавления клиентской машины в домен.

Методические материалы, определяющие процедуру оценивания выполнения практических работ

Описание методики оценивания выполнения практических работ: оценка за выполнение тестовых заданий ставится на основании знания теоретического материала по теме практической работы, умений и навыков применения знаний на практике, работы с оборудованием, анализировать результаты практической работы.

Критерии оценки (в баллах*):*

- **5** баллов выставляется студенту, если демонстрируются знания темы, цели и задач практической работы, хода работы, применяемых методик исследования; демонстрируется полное знание теоретического материала по теме практической работы (в процессе обсуждения, при ответе на контрольные вопросы); демонстрируются умения и навыки работы с оборудованием, применения знания на практике, анализа результатов практической работы и формулирование выводов, владение навыками прикладной деятельности;
- **4** балла выставляется студенту, если демонстрируются знания темы, цели и задач практической работы, хода работы, имеются пробелы в знании применяемых методик исследования; демонстрируется неполное знание фактического материала по теме практической работы (в процессе обсуждения, при ответе на контрольные вопросы); демонстрируются некоторые недостатки умения работать с оборудованием, применять знания на практике, недостатки владения

навыками прикладной деятельности и способности анализировать результаты практической работы, формулировать выводы, прослеживать причинно-следственные связи;
- **3** балла выставляется студенту, если демонстрируются неполные знания цели и задач практической работы, хода работы, применяемых методик исследования; демонстрируется неполное, несистемное знание теоретического материала по теме практической работы (в процессе обсуждения, при ответе на контрольные вопросы); демонстрируются заметные недостатки в умении работать с оборудованием, применять знания на практике, недостаточно владеет навыками прикладной деятельности, способностью анализировать результаты практической работы и формулировать выводы, прослеживать причинно-следственные связи;
- **0**-**2** балла выставляется студенту, если демонстрируются полное или почти полное отсутствие знания цели и задач практической работы, хода работы, применяемых методик исследования; демонстрируется полное или почти полное отсутствие знания теоретического материала по теме практической работы (в процессе обсуждения, при ответе на контрольные вопросы); демонстрируются значительные недостатки умения работать с оборудованием, применять знания на практике, владения навыками прикладной деятельности, способности анализировать результаты практической работы и формулировать выводы, прослеживать причинно-следственные связи.

Групповой опрос

Примеры вопросов:

1. Уровни формирования режима информационной безопасности
2. Нормативно-правовые основы информационной безопасности в РФ
3. Ответственность за нарушения в сфере информационной безопасности
4. Антивирусные программы
5. Правила защиты от компьютерных вирусов
6. Специфика средств защиты в компьютерных сетях

Методические материалы, определяющие процедуру оценивания группового вопроса

В процессе проведения занятия задаются вопросы по темам, как текущего занятия, так и по предыдущим.
Студент, правильно отвечающий на вопрос, получает дополнительный балл.
Студент, неправильно ответивший на вопрос, не получает дополнительный балл.

Лабораторная работа

Лабораторная работа № 4

1.1 Постановка задачи
Используя стандартные сетевые утилиты, проанализировать конфигура-цию сети на платформе ОС Windows, т.е. получить свой IP-адрес, узнать имя домена, имена компьютеров, входящих в домен, просмотреть и при необходи-мости подключить общие ресурсы, определить причину возможных неполадок, так же получить информацию об использовании портов.

1.2 Краткая теоретическая справка
Мониторинг и анализ сети представляют собой важные этапы контроля работы сети. Для решения этих задач регулярно производится сбор данных, ко-торый дает базу для измерения реакции сети на изменения и перегрузки. Чтобы осуществить сетевую передачу, нужно проверить корректность подключения клиента к сети, наличие у клиента хотя бы одного протокола сервера, знать IP-адрес компьютеров сети и т. д. Поэтому в сетевых операционных системах, и в частности, в Windows, существует множество мощных утилит для пересылки текстовых сообщений, управления общими ресурсами, диагностике сетевых подключений, поиска и обработки ошибок.
Утилиты запускаются из командной строки или из сеанса MS DOS!

1.3 Сетевые утилиты

1.3.1 Утилита hostname

Выводит имя локального компьютера (хоста). Она доступна только после установки поддержки протокола TCP/IP. Пример вызова команды *host-name*1*)*:
G:\UTILl>hostname
14423-5

1.3.2 Утилита ipconfig

Выводит диагностическую информацию о конфигурации сети TCP/IP. Эта утилита позволяет просмотреть текущую конфигурацию IP-адресов ком-пьютеров сети. Синтаксис утилиты *ipconfig*:
ipconfig [/*all* | */renew* [адаптер] | */release* [адаптер]],
где
all - выводит сведения о имени хоста, DNS (Domain Name Service), типе узла, IP-маршрутизации и др. Без этого параметра команда *ipconfig* выводит только IP-адреса, маску подсети и основной шлюз;
/renew [адаптер] - обновляет параметры конфигурации DHCP (Dynamic Host Configuration Protocol – автоматическая настройка IP-адресов). Эта возможность доступна только на компьютерах, где запущена служба клиента DHCP. Для задания адаптера используется имя, выводимое командой *ipconfig* без параметров;
/release [адаптер] - очищает текущую конфигурацию DHCP. Эта возможность отключает TCP/IP на локальных компьютерах и доступна только на клиентах DHCP. Для задания адаптера используется имя, выводимое командой *ipconfig* без параметров. Эта команда часто используется перед перемещением компьютера в другую сеть. После использования утилиты *ipconfig /release*, IP-адрес становиться доступен для назначения другому компьютеру.
Запущенная без параметров, команда *ipconfig* выводит полную конфигурацию TCP/IP, включая IP адреса и маску подсети.
Примеры использования *ipconfig* без параметров и с ключом */all*:
- без параметров:
C:\Program Files>ipconfig
Настройка протокола IP для Windows 2000
Адаптер Ethernet Подключение по локальной сети:
DNS суффикс этого подключения :
IP – адрес : 192.168.144.235
Маска подсети : 255.255.248.0
Основной шлюз : 192.168.144.211
- с ключом */all*
Настройка протокола IP для Windows 2000
Имя компьютера : 14423-5
Основной DNS суффикс : FIT.local
Тип узла : Широковещательный
Включена IP-маршрутизация : Нет
Доверенный WINS-сервер : Нет
Порядок просмотра суффиксов DNS : FIT.local
Адаптер Ethernet Подключение по локальной сети:
DNS суффикс этого подключения
Описания
Физический адрес : 00-02-44-12-07-A7
DHCP разрешен : Нет
IP-адрес : 192.168.144.235

Маска подсети : 255.255.248.0
Основной шлюз : 192.168.144.211
DNS-серверы : 192.168.144.211

1.3.3 Утилита net view

Просматривает список доменов, компьютеров или общих ресурсов на данном компьютере. Синтаксис утилиты *net view*:
net view [*компьютер* | */domain*[:домен]];
net view /network:nw [\\компьютер] – используется в сетях Novell NetWare,
где *компьютер* - задает имя компьютера для просмотра общих ресурсов;
/domain[:домен] - задает домен, для которого выводится список компьютеров. Если параметр не указан, выводятся сведения обо всех доменах в сети;
/network:nw - выводит все доступные серверы в сети Novell NetWare. Если указано имя компьютера, выводится список его ресурсов в сети Net-Ware. С помощью этого ключа могут быть просмотрены ресурсы и в других локальных сетях.
Вызванная без параметров, утилита выводит список компьютеров в текущем домене.
Пример использования утилиты *net view*:
- без параметров:
C:\Program Files\Far>net view
Имя сервера Заметки

\\14404-1
\\14422-1
\\14422-2
\14422-3
\\14423-10
\\14423-2
\\14423-3
\\14423-4
\\14423-5
\\14423-6
\\14423-7
\\14423-8
\\14423-9
\\14424-2 USER
\\FIT-S1
Команда выполнена успешно
- с параметром *компьютер*:
C:\program Files\Far>net view 14423-8
Общие ресурсы на 14423-8

Сетевое имя Тип Использовать как Комментарий
---
hdd_c Диск
hdd_d Диск
Команда выполнена успешно.

1.3.4 Утилита ping

Проверяет соединения с удаленным компьютером или компьютерами. Эта команда доступна только после установки поддержки протокола TCP/IP. Синтаксис утилиты *ping*:

ping [*-t*] [*-a*] [*-n счетчик*] [*-l длина*] [*-f*] [*-i ttl*] [*-v тип*] [*-r счетчик*] [*-s число*] [[*-j список_комп*] | [*-k список_комп*]] [*-w интервал*] *спи-сок_назн*,
где *-t* - повторяет запросы к удаленному компьютеру, пока программа не будет остановлена;
-a - разрешает имя компьютера в адрес;
-n счетчик - передается число пакетов ECHO, заданное параметром. По умолчанию – 4;
-l длина - отправляются пакеты типа ECHO, содержащие порцию данных заданной длины. По умолчанию - 32 байта, максимум – 65527;
-f - отправляет пакеты с флагом запрещения фрагментации (Do not Fragment). Пакеты не будут разрываться при прохождении шлюзов на своем маршруте;
-i ttl - устанавливает время жизни пакетов TTL (Time To Live);
-v тип - устанавливает тип службы (Type Of Service) пакетов;
-r счетчик - записывает маршрут отправленных и возвращенных пакетов в поле записи маршрута Record Route. Параметр счетчик задает число компьютеров в интервале от 1 до 9;
-s число - задает число ретрансляций на маршруте, где делается отметка времени;
-j список_комп - направляет пакеты по маршруту, задаваемому парамет-ром список_комп. Компьютеры в списке могут быть разделены промежуточными шлюзами (свободная маршрутизация). Максимальное количество, разрешаемое протоколом IP, равно 9;
-k список_комп - направляет пакеты по маршруту, задаваемому параметром список_комп. Компьютеры в списке не могут быть разделены промежуточными шлюзами (ограниченная маршрутизация). Максимальное количество, разрешаемое протоколом IP, равно 9;
-w интервал - указывает промежуток времени ожидания (в миллисекундах);

список_назн - указывает список компьютеров, которым направляются запросы;
Пример использования утилиты *ping* с параметром *список_назн*:
C:\Program Files\Far>ping 14423-8
Обмен пакетами с 14423-8.FIT.local [192.168.144.238] по 32 байт
Ответ от 192.168.144.238: число байт=32 время<10мс TTL=128
Ответ от 192.168.144.238: число байт=32 время<10мс TTL=128
Ответ от 192.168.144.238: число байт=32 время<10мс TTL=128
Ответ от 192.168.144.238: число байт=32 время<10мс TTL=128
Статистика Ping для 192.168.144.238:
Пакетов: отправлено =4 , получено = 4, потеряно = 0(0% потерь)
Приблизительное время передачи и приема:
наименьшее = 0мс, наибольшее= 0мс, среднее = 0мс

1.3.5 Утилита netstat

Выводит статистику протокола и текущих подключений сети TCP/IP. Эта команда доступна только после установки поддержки протокола TCP/IP.
Синтаксис утилиты *netstat*:
netstat [*-a*] [*-e*] [*-n*] [*-s*] [*-p протокол*] [*-r*] [*интервал*],
где *-a* - выводит все подключения и сетевые порты. Подключения сервера обычно не выводятся;
-e - выводит статистику Ethernet. Возможна комбинация с ключом *–s*;
-n - выводит адреса и номера портов в шестнадцатеричном формате (а не имена);
-s - выводит статистику для каждого протокола. По умолчанию выводится статистика для TCP, UDP, ICMP (Internet Control Message Protocol) и IP. Ключ *-p* может быть использован для указания подмножества стан-дартных протоколов;
-p протокол - выводит соединения для протокола, заданного парамет-ром. Параметр может иметь значения *tcp* или *udp*. Если используется с ключом *-s* для вывода статистики по отдельным протоколам, то пара-метр может принимать значения *tcp*, *udp*, *icmp* или *ip*;
-r - выводит таблицу маршрутизации;

интервал - обновляет выведенную статистику с заданным в секундах интервалом. Нажатие клавиш CTRL+B останавливает обновление стати-стики. Если этот параметр пропущен, *netstat* выводит сведения о теку-щей конфигурации один раз.
Пример использования *netstant*:

- без параметров:
C:\Program Files\Far\netstat
Активные подключения
Имя Локальный адрес Внешний адрес Состояние
TCP 14423-5:1245 14423-3:netbios-ssn ESTABLISHED
- с параметром -*a*:
C:\Program Files\Far>netstat –a
Активные подключения
Имя Локальный адрес Внешний адрес Состояние
TCP 14423-5:epmap 14423-5:FIT.local:0 LISTENING
TCP 14423-5:microsoft-ds 14423-5:FIT.local:0 LISTENING
TCP 14423-5:1049 14423-5:FIT.local:0 LISTENING
TCP 14423-5:1072 14423-5:FIT.local:0 LISTENING
TCP 14423-5:netbios-ssn 14423-5:FIT.local:0 LISTENING
TCP 14423-5:427 14423-5:FIT.local:0 LISTENING
TCP 14423-5:1245 14423-3:netbios-ssn TIME_WAIT
UDP 14423-5:epmap *:*
UDP 14423-5:microsoft-ds *:*
UDP 14423-5:1026 *:*
UDP 14423-5:1043 *:*
UDP 14423-5:1051 *:*
UDP 14423-5:netbios-ssn *:*
UDP 14423-5:netbios-dgm *:*
UDP 14423-5: 427 *:*
UDP 14423-5:isakmp *:*
UDP 14423-5:1048 *:*

1.3.6 Утилита tracert

Диагностическая утилита, предназначенная для определения маршрута до точки назначения с помощью посылки эхо-пакетов протокола ICMP с раз-личными значениями срока жизни (TTL, Time-To-Live). При этом требуется, чтобы каждый маршрутизатор на пути следования пакетов уменьшал эту вели-чину по крайней мере на 1 перед дальнейшей пересылкой пакета. Это делает параметр TTL эффективным счетчиком числа ретрансляций. Предполагается, что когда параметр TTL становится равен 0, маршрутизатор посылает системе-источнику сообщение ICMP «Time Exceeded». Утилита *tracert* определяет мар-шрут путем посылки первого эхо-пакета с параметром TTL, равным 1, и с по-следующим увеличением этого параметра на единицу до тех пор, пока не будет получен ответ из точки назначения или не будет достигнуто максимальное до-пустимое значение TTL. Маршрут определяется проверкой сообщений ICMP «Time Exceeded», полученных от промежуточных маршрутизаторов. Однако некоторые маршрутизаторы сбрасывают пакеты с истекшим временем жизни без отправки соответствующего сообщения. Эти маршрутизаторы невидимы для утилиты *tracert*. Синтаксис утилиты *tracert*:

tracert [-*d*] [-*h макс_узл*] [-*j список_компьютеров*] [-*w интервал*] *точка_назн*,
где -*d* - отменяет разрешение имен компьютеров в их адреса;

-h макс_узл - задает максимальное количество ретрансляций, используе-мых при поиске точки назначения;
-j список_компьютеров - задает список_компьютеров для свободной маршрутизации;
-w интервал - задает интервал в миллисекундах, в течение которого бу-дет ожидаться ответ;
точка_назн - указывает имя конечного компьютера.
Пример использования утилиты *tracert*:
T:\>tracert 14423-7
Трассировка маршрута к 14423-7.FIT.local [192.168.144.237]
С максимальным числом прыжков 30:
1 <10мс <10мс <10мс 14423-7 [192.168.144.237]
Трассировка завершена

1.3.7 Утилита net use

Подключает общие сетевые ресурсы или выводит информацию о под-ключениях компьютера. Команда также управляет постоянными сетевыми со-единениями. Синтаксис утилиты *net use*:
net use [*устройство* | *] [*компьютер**ресурс*[*том*]] [*пароль* | *]] [*/user:*[*домен*\]*имя_пользователя*] [[*/delete*] | [*/persistent:{yes* | *no}*]]
net use устройство [*/home*[*пароль* | *]] [*/delete:{yes* | *no}*]
net use [*/persistent:{yes* | *no}*],
где *устройство* - задает имя ресурса при подключении/отключении. Существует два типа имен устройств: дисководы (от D: до Z:) и принте-ры (от LPT1: до LPT3:). Ввод символа звездочки обеспечит подключе-ние к следующему доступному имени устройства;
*компьютер**ресурс* - указывает имя сервера и общего ресурса. Если па-раметр компьютер содержит пробелы, все имя компьютера от двойной обратной черты (\\) до конца должно быть заключено в кавычки (" "). Имя компьютера может иметь длину от 1 до 15 символов;
том - задает имя тома системы Novell NetWare. Для подключения к серверам Novell NetWare должна быть запущена служба клиента сети Novell NetWare (для Windows 2000 Professional) или служба шлюза сети Novell NetWare (для Windows 2000 Server);
пароль - задает пароль, необходимый для подключения к общему ресур-су;
* - выводит приглашение для ввода пароля. При вводе с клавиатуры символы пароля не выводятся на экран;
/user - задает другое имя пользователя для подключения к общему ре-сурсу;
домен - задает имя другого домена. Если домен не указан, используется текущий домен;
имя_пользователя - указывает имя пользователя для подключения;
/delete - отменяет указанное сетевое подключение. Если подключение задано с символом звездочки, будут отменены все сетевые подключения;
/home - подключает пользователя к его основному каталогу;
/persistent - управляет постоянными сетевыми подключениями. По умолчанию берется последнее использованное значение. Подключения без устройства не являются постоянными;
yes - сохраняет все существующие соединения и восстанавливает их при следующем подключении;
no - не сохраняет выполняемые и последующие подключения. Сущест-вующие подключения восстанавливаются при следующем входе в сис-тему. Для удаления постоянных подключений используется ключ */delete*.
Вызванная без параметров утилита *net use* извлекает список сетевых подключений.
Пример использования *net use*:
C:\Program Files>net use t: \\fit-s1\install
Команда выполнена успешно

1.3.8 Утилита net send

Отправка сообщения другому пользователю, компьютеру или псевдони-му в сети. Служба сообщений должна быть запущена на компьютере для полу-чения сообщений. Синтаксис утилиты *net send*:
*net send {имя | * | /domain*[*:имя*] | */users} сообщение,*
где *имя* - указывает имя пользователя, имя компьютера или псевдоним, которому будет отправлено сообщение. Если имя компьютера содержит пробелы, оно должно быть заключено в кавычки (" "). Длинные имена пользователей, введенные в формате NetBIOS, могут привести к возник-новению исключительных ситуаций. Имена NetBIOS ограничены 16 символами, но Windows 2000 резервирует 16-ый символ;
* - отправляет сообщение всем членам группы;
/domain[*:имя*] - отправляет сообщение всем именам в домене компьюте-ра. Если параметр имя указан, сообщение будет отправлено всем именам заданного домена или рабочей группы;
/users - отправляет сообщение всем пользователям, подключенным к серверу;

сообщение - указывает текст сообщения.
Пример использования *net send*:
T:\netsend 14423-8 проверка связи
Сообщение успешно отправлено 14423-8

1.4 Рекомендации и замечания

На основе рассмотренных сетевых утилит ОС Windows разрабатываются пользовательские приложения, реализующие мониторинг и диагностику ло-кальных сетей. Они позволяют минимизировать усилия по поиску и исправле-нию ошибок в конфигурации сети и помогают системному администратору контролировать трафик. В настоящее время создано большое количество про-грамм этого направления: Monitor It, Nautilus NetRanger, CiscoWorks 2000, ServiceSentinel и д.р. Они распространяются через Internet на условиях freeware. Windows NT Server обладает встроенными инструментами мониторинга: Event Viewer, Performance Monitor, Network Monitor.

1.5 Контрольные вопросы

1.5.1 Исправить синтаксис утилиты. C:\Program Files\Far\>net view all.
1.5.2 Для чего нужна утилита net send? Описать ее синтаксис.
1.5.3 Укажите неверный параметр C:\net use B:\\fit-s1\:install.
1.5.4 Можно ли утилитой tracert задать максимальное число ретрансляций?
1.5.5 Какой протокол необходим для работы с утилитой ping?
1.5.6 Какой результат выдаст утилита net stat с параметрами –a s –r?
1.5.7 Для чего необходима утилита hostname?
1.5.8 Зачем используется параметр all в утилите ipconfig?

Методические материалы, определяющие процедуру оценивания выполнения лабораторных работ

Описание методики оценивания выполнения лабораторных работ: оценка за выполнение ЛР ставится на основании знания теоретического материала по теме лабораторной работы, умений и навыков применения знаний на практике, работы с оборудованием, анализа результатов лабораторной работы.
Критерии оценки (в баллах*):*
- **5** баллов выставляется студенту, если демонстрируются знания темы, цели и задач лабораторной работы, хода работы, применяемых методик исследования; демонстрируется полное знание теоретического материала по теме лабораторной работы (в процессе обсуждения, при ответе на контрольные вопросы); демонстрируются умения и навыки работы с оборудованием, применения знания на практике, анализа результатов лабораторной работы и формулирование выводов, владение навыками прикладной деятельности;
- **4** балла выставляется студенту, если демонстрируются знания темы, цели и задач лабораторной работы, хода работы, имеются пробелы в знании применяемых методик исследования;

демонстрируется неполное знание фактического материала по теме лабораторной работы (в процессе обсуждения, при ответе на контрольные вопросы); демонстрируются некоторые недостатки умения работать с оборудованием, применять знания на практике, недостатки владения навыками прикладной деятельности и способности анализировать результаты лабораторной работы, формулировать выводы, прослеживать причинно-следственные связи;
- **3** балла выставляется студенту, если демонстрируются неполные знания цели и задач лабораторной работы, хода работы, применяемых методик исследования; демонстрируется неполное, несистемное знание теоретического материала по теме лабораторной работы (в процессе обсуждения, при ответе на контрольные вопросы); демонстрируются заметные недостатки в умении работать с оборудованием, применять знания на практике, недостаточно владеет навыками прикладной деятельности, способностью анализировать результаты лабораторной работы и формулировать выводы, прослеживать причинно-следственные связи;
- **0-2** балла выставляется студенту, если демонстрируются полное или почти полное отсутствие знания цели и задач лабораторной работы, хода работы, применяемых методик исследования; демонстрируется полное или почти полное отсутствие знания теоретического материала по теме лабораторной работы (в процессе обсуждения, при ответе на контрольные вопросы); демонстрируются значительные недостатки умения работать с оборудованием, применять знания на практике, владения навыками прикладной деятельности, способности анализировать результаты лабораторной работы и формулировать выводы, прослеживать причинно-следственные связи.

Зачет

Зачет является оценочным средством для всех этапов освоения компетенций.

Примерные вопросы к зачету, 2 курс / 4 семестр

1. Понятие информации, ее свойства.
2. Надежность информации.
3. Понятие информационного ресурса.
4. Классификация информационных ресурсов
5. Информационные ресурсы в современных условиях.
6. Понятие об информационной безопасности.
7. Категории информационной безопасности.
8. Информационная безопасность человека и общества.
9. Методы обеспечения информационной безопасности.
10. Правовое обеспечение информационной безопасности в РФ.
11. Основные угрозы информационной безопасности для государства, человека, информационной системы.
12. Защита информации. Основные понятия, направления организации защиты информации.
13. Характеристика основных методов защиты информации.
14. Организационные меры защиты информации.
15. Программно-технические меры защиты информации.
16. Правовые меры защиты информации.
17. Практика применения методов и средств защиты информации.
18. Характеристика основных средств защиты информации.
19. Угрозы компьютерной безопасности.
20. Типы вредоносных программ. Борьба с ними.
21. Защита операционных систем.
22. Защита программного обеспечения.
23. Аутентификация пользователей.

Методические материалы, определяющие процедуру оценивания зачета

Зачет выставляется по рейтингу, в зависимости от эффективности работы в процессе изучения дисциплины, что определяется количеством набранных баллов за все виды заданий текущего и рубежного контроля
зачтено – от 60 до 110 баллов
не зачтено – от 0 до 59 баллов.

Задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме:

4 семестр - зачет.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины.

Для проверки *знаний* используются вопросы и задания в различных формах.

Умения, навыки (или опыт деятельности) и компетенции проверяются с помощью компетентностно-ориентированных задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов.

Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине при использовании модульно-рейтинговой системы

Критериями оценивания при модульно-рейтинговой системе являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины:

для зачета: текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10.

Шкалы оценивания:

для зачета:

зачтено – от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),

не зачтено – от 0 до 59 рейтинговых баллов.

Рейтинг-план дисциплины

Таблица перевода баллов текущего контроля в баллы рейтинга

	5	**5**	**5**	**5**	**5**	**5**	**5**	**5**	**5**	**5**
0	0	0	0	0	0	0	0	0	0	0
1	5	3	2	2	1	1	1	1	1	1
2		5	4	3	2	2	2	2	2	1
3			5	4	3	3	3	2	2	2
4				5	4	4	3	3	3	2

5					5	5	4	4	3	3
6						5	5	4	4	3
7							5	5	4	4
8								5	5	4
9									5	5
10										5

Рейтинг-план дисциплины представлен в Приложении 1.

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

5.1. Основная учебная литература

1. Информационная безопасность : Учеб. для студ. вузов, обуч. по гуман. и соц .-эконом. спец. / В. И. Ярочкин .— 5-е изд. — М. : Гаудеамус: Академический Проект, 2008 .— 543 с.
2. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях : учеб. пособие — Электрон. дан. — М.: ДМК Пресс, 2012. — 592 с. — Режим доступа: https://e.lanbook.com/book/3032
3. Информационная безопасность [Электронный ресурс] : учебник для вузов / В. Ф. Шаньгин . — Москва : ДМК Пресс, 2014 .— 702 с. : ил. — Доступ к тексту электронного издания возможен через Электронно-библиотечную систему "Лань" .— <URL:https://e.lanbook.com/book/50578#book_name>.

5.2. Дополнительная учебная литература

1. Нечаев, Д.Ю. Надежность информационных систем [Электронный ресурс] : учебное пособие / Д.Ю. Нечаев, Ю.В. Чекмарев. — Электрон. дан. — Москва : ДМК Пресс, 2012. — 64 с. — Режим доступа: https://e.lanbook.com/book/3030
2. Информационная безопасность компьютерных систем и сетей: учеб. пособ. для студ. учрежд. сред. проф. образ., обуч. по группе спец. 2200 "Информатика и вычислит. техника" / В. Ф. Шаньгин .— М. : Форум: ИНФРА-М, 2010 .— 415 с.

5.3. Другие учебно-методические материалы

Перечень рекомендуемых ресурсов информационно-телекоммуникационной сети «Интернет», находящихся в свободном доступе

1. http://www.inside-zi.ru/ - Журнал «Защита информации. Инсайд»

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины

1. Научная электронная библиотека eLIBRARY.RU [Электронный ресурс]. – Режим доступа: https://elibrary.ru/.
2. Электронная библиотечная система «Лань» [Электронный ресурс]. – Режим доступа: https://

e.lanbook.com/.

3. Университетская библиотека онлайн biblioclub.ru [Электронный ресурс]. – Режим доступа: http://biblioclub.ru/.
4. Электронная библиотека УУНиТ [Электронный ресурс]. – Режим доступа: https://elib.bashedu.ru/.
5. Российская государственная библиотека [Электронный ресурс]. – Режим доступа: https://www.rsl.ru/.
6. Национальная электронная библиотека [Электронный ресурс]. – Режим доступа: https://xn--90ax2c.xn--p1ai/viewers/.
7. Национальная платформа открытого образования npoed.ru [Электронный ресурс]. – Режим доступа: http://npoed.ru/.
8. Электронное образование Республики Башкортостан [Электронный ресурс]. – Режим доступа: https://edu.bashkortostan.ru/.
9. Информационно-правовой портал Гарант.ру [Электронный ресурс]. – Режим доступа: http://www.garant.ru/.

Программное обеспечение

1. Браузер Яндекс - Бесплатная лицензия https://yandex.ru/legal/browser_agreement/index.html
2. Visual Studio Community - Бесплатная лицензия https://visualstudio.microsoft.com/ru/free-developer-offers/
3. LIBREOFFICE - Договор №0301400003023000002 от 14.03.2023 (бессрочный)
4. Операционная система Astra Linux - Договор 0301400003023000002 от 14 марта 2023 бессрочно
5. Система дистанционного обучения Moodle - Бесплатная лицензия http://www.gnu.org/licenses/gpl.html
6. Справочная Правовая Система "КонсультантПлюс" - Договор №125818-С от 28.04.2026
7. Программа моделирования сетей NetEmul - Бесплатная лицензия http://netemul.sourceforge.net/help/en/intro.html
8. Программа для симулирования и планирования сети GraphicalNetworkSimulator 3 - Бесплатная лицензия https://docs.gns3.com/1PvtRW5eAb8RJZ11maEYD9_aLY8kkdhgaMB0wPCz8a38/index.html
9. Файловый менеджер DoubleCommander - Бесплатная лицензия https://sourceforge.net/projects/doublecmd/

7. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
Аудитория 311(ФМ)	Лекционная, Семинарская, Для консультаций, Для контроля и аттестации, Для лабораторных занятий, Для практических занятий	Доска, компьютер, мебель, проектор, экран. Программное обеспечение 1. Браузер Яндекс 2. Visual Studio Community 3. Система дистанционного

		обучения Moodle 4. Программа моделирования сетей NetEmul 5. Программа для симулирования и планирования сети GraphicalNetworkSimulator 3 6. Операционная система Astra Linux 7. LIBREOFFICE
Аудитория 311 а(ФМ)	Для хранения оборудования	Компьютер, мебель. Программное обеспечение 1. Операционная система Astra Linux 2. LIBREOFFICE
Аудитория 313(ФМ)	Лекционная, Семинарская, Для консультаций, Для контроля и аттестации, Для лабораторных занятий, Для практических занятий	Доска, компьютер, мебель, принтер, проектор, экран. Программное обеспечение 1. Visual Studio Community 2. LIBREOFFICE 3. Файловый менеджер DoubleCommander 4. Программа моделирования сетей NetEmul 5. Программа для симулирования и планирования сети GraphicalNetworkSimulator 3 6. Операционная система Astra Linux 7. Браузер Яндекс
Аудитория 411(ФМ)	Лекционная, Семинарская, Для консультаций, Для контроля и аттестации	Компьютер, мебель, проектор, экран. Программное обеспечение 1. Visual Studio Community 2. Операционная система Astra Linux 3. LIBREOFFICE 4. Файловый менеджер DoubleCommander 5. Программа моделирования сетей NetEmul 6. Программа для симулирования и планирования сети GraphicalNetworkSimulat

		or 3 7. Браузер Яндекс
Аудитория 420(ФМ)	Для самостоятельной работы	Компьютер, мебель, нетбук, принтер. Программное обеспечение 1. Visual Studio Community 2. LIBREOFFICE 3. Операционная система Astra Linux
Аудитория 422(ФМ)	Лекционная, Семинарская, Для консультаций, Для контроля и аттестации, Для лабораторных занятий, Для практических занятий	Доска, компьютер, мебель, ноутбук, проектор. Программное обеспечение 1. Visual Studio Community 2. LIBREOFFICE 3. Браузер Яндекс 4. Программа для симулирования и планирования сети GraphicalNetworkSimulator 3 5. Программа моделирования сетей NetEmul
Аудитория 422 а(ФМ)	Для хранения оборудования	Камера web creative live, ноутбук, проектор, радиомикрофонная система с петличным микрофоном, фотокамера. Программное обеспечение 1. LIBREOFFICE 2. Операционная система Astra Linux
Читальный зал(ФМ)	Для самостоятельной работы	Компьютер, мебель, принтер, учебно-методические материалы. Программное обеспечение 1. Справочная Правовая Система "КонсультантПлюс" 2. Браузер Яндекс 3. LIBREOFFICE 4. Операционная система Astra Linux