МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ
Заведующий кафедрой
функционального анализа
и операторных уравнений

Каменский М.И.
подпись, расшифровка подписи

26.06.2018 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.Б.30 Безопасность сетей ЭВМ

1. Код и наименование направления подготовки/специальности: 10.05.04 Информационно-аналитические системы безопасности

2. Профиль подготовки/специализация:

3. Квалификация (степень) выпускника: специалист

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины: функционального анализа и операторных уравнений

6. Составители программы: Ушаков Сергей Николаевич, канд. физ-мат. наук

7. **Рекомендована:** НМС математического факультета, протокол №0500-07 от 03.07.2018

8. Учебный год:2018-2019 **Семестр(ы):** 4,5

9. Цели и задачи учебной дисциплины:

Цель курса – формирование у студентов компетентности в области информационной безопасности сетей ЭВМ; изучение методов и средств обеспечения защиты информации при передаче ее по каналам связи от нарушения конфиденциальности, целостности и доступности информации.

Основными задачами изучения дисциплины являются:

- изучение базовой инфраструктуры сетей ЭВМ, основных устройств и систем, требований к обеспечению информационной безопасности, соответствующих стандартов, технических спецификаций, протоколов и технологий;
- формирование умений по созданию, настройке и эксплуатации безопасных сетей ЭВМ
- овладение навыками по использованию компонентов защищенных сетей ЭВМ, способностью разрабатывать модели угроз и модели нарушителей ИБ на основе исходных данных о сети

В результате освоения дисциплины обучающийся должен:

знать:

- базовую инфраструктуру сетей ЭВМ, основных ее устройств и систем;
- основные направления развития информационно-коммуникационных технологий объекта защиты,
- методы оценки эффективности функционирования систем информационной безопасности, способы оценки затрат и рисков;
- типовые структуры, принципы организации, средства и технологии обеспечения информационной безопасности объектов защиты
- современные методы обеспечения информационной безопасности, вновь вводимые отечественные и международные стандарты;
- - основные угрозы информационной безопасности объектов и методы противодействия им;
- требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования;
- нормативные документы по метрологии, стандартизации и сертификации программных и аппаратных средств защиты.
- структуры и организацию построения узлов защищенных компьютерных телекоммуникационных сетей;
- методы обеспечения надежности защищенных компьютерных телекоммуникационных сетей;
- основные методы криптографической защиты информации;

уметь:

- использовать полученные знания для организации безопасной работы сетей ЭВМ;
- анализировать и выявлять угрозы и уязвимости информационных телекоммуникационных систем, определять источники этих угроз, их способы реализации и цели;
- защищать ресурсы сетей ЭВМ от вредоносных программ и их вредного воздействия;

- оценить защищенность сетей ЭВМ;
- программировать алгоритмы криптографической защиты информации в компьютерных сетях.

владеть:

- навыками проектирования системы защиты сетей ЭВМ, обеспечивающей сохранность целостности и авторства передаваемых сообщений, защиты от несанкционированного доступа к передаваемой информации;
- навыками работы со специализированным программно-аппаратным обеспечением безопасности компьютерных сетей.

10. Место учебной дисциплины в структуре ООП:

Дисциплина входит в базовую часть профессионального цикла. Для изучения и освоения дисциплины нужны знания из предшествующих курсов: Дискретная математика, Информатика, Математическая логика и теория алгоритмов, Языки программирования, Технология и методы программирования, Основы информационной безопасности. Знания и умения, приобретенные студентами в результате изучения дисциплины, будут использоваться при изучении курсов: Безопасность операционных систем, Безопасность электронного документооборота, Безопасность информационных и аналитических систем, Моделирование автоматизированных информационных систем, Принципы построения, проектирования и эксплуатации автоматизированных информационных систем, Безопасность программного обеспечения, а также при выполнении курсовых и дипломных работ, связанных с математическим моделированием в области информационной безопасности и защиты информации.

11. Компетенции обучающегося, формируемые в результате освоения дисциплины:

Компетенция		Планируемые результаты обучения
Код	Название	
ПК-9	способностью выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах	знать: как выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах уметь: выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах владеть (иметь навык(и)): способностью выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах

ПК-15	способность эксплуатировать специальные ИАС и средства обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстанавливать их работоспособность при внештатных ситуациях	знать: специальные ИАС и средства обеспечения их информационной безопасности на всех этапах жизненного цикла уметь: эксплуатировать специальные ИАС и средства обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстанавливать их работоспособность при внештатных ситуациях владеть: способностью эксплуатировать специальные ИАС и средства обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстанавливать их работоспособность при внештатных ситуациях
ОПК-7	способность применять методы и средства обеспечения информационной безопасности специальных ИАС	знать: сущность и понятие информации, информационной безопасности и характеристику ее составляющих; место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России; основные свойства информации (ценность, целостность, конфиденциальность, доступность); задачи информационной безопасности; источники и классификацию угроз информационной безопасности, каналы несанкционированного доступа к информации, основные угрозы доступности, целостности и конфиденциальности информации; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; уровни формирования режима информационной безопасности; правовые основы информационной безопасности; цели и задачи организационно-административного уровня обеспечения информационной безопасности; технические средства обеспечения информационной безопасности; программно-аппаратные средства обеспечения информационной безопасности; основные методы криптографической защиты информации; методы защиты информации в вычислительных сетях; принципы функционирования компьютерных вирусов и методы борьбы с ними; уметь: использовать полученные знания для организации безопасной работы персональных компьютеров; выявлять угрозы информационной

		безопасности, определять источники этих угроз, их способы реализации и цели; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; правомерно использовать организационные, технические и программно-аппаратные средства защиты информации; защищать ресурсы персональных компьютеров и сетуй на их основе от компьютерных вирусов и их вредного воздействия; оценить защищенность информационных систем; владеть (иметь навык(и))**:** профессиональной терминологией в области информационной безопасности; навыками работы со специальной литературой; навыками работы со специализированным программно-аппаратным обеспечением компьютерной безопасности.

12. Объем дисциплины в зачетных единицах/часах в соответствии с учебным планом — 6/216

Форма промежуточной аттестации: зачет, экзамен.

12.2 Виды учебной работы:

Вид учебной работы	Трудоемкость (часы)		
	Всего	По семестрам	
		сем. № 4	сем. № 5
Аудиторные занятия	*118*	*50*	*68*
в том числе: лекции	*68*	*34*	34
практические	-	-	-
лабораторные	*50*	*16*	34
Самостоятельная работа	*62*	*22*	40
Контроль	*36*	-	36
Форма промежуточной аттестации		*1 контрольная работа, зачет*	*2 контрольные работы, экзамен*
Итого:	*216*	*72*	*144*

13.1. Содержание разделов дисциплины:

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1	Основные понятия компьютерных сетей. Определение локальных сетей и их топология	Основные понятия компьютерных сетей. История компьютерных сетей. Типы сетевых архитектур. Типы серверов. Отличия сетевых топологий. Требования, предъявляемые к современным вычислительным сетям.
2	Типы линий связи локальных сетей. Подключение линий связи и коды передачи информации	Типы, особенности, принципы функционирования, правила использования линий связи, применяемых в локальных сетях. Принципы подключения электрических линий связи в локальных сетях, методах их согласования, а также о кодах передачи информации. Методы цифрового кодирования. Способы модуляции
3	Пакеты, протоколы. Методы управления обменом	Принципы передачи информации по сети. Назначение и типы информационных пакетов, структура пакетов. Методы управления обменом в сетях с разной топологией. Стандартные стеки коммуникационных протоколов. Способы разделения канала по частоте и времени.
4	Сетевая модель OSI	Стандартная модель взаимодействия открытых систем OSI, уровни функций, выполняемых при взаимодействии по сети. Возможности сетевых адаптеров и промежуточных сетевых устройств. Функции модели OSI, реализуемых программно, стандартные протоколы обмена, их достоинствах и недостатках, типы сетевых программных средств и особенности сетевых программ крупнейших производителей. Принципы работы протоколов разных уровней
5	Физический уровень модели OSI. Технология Ethernet	Характеристики линий связи. Типы кабелей. Коннекторы. Модуляция. Методы кодирования. Формат кадра Ethernet. Передача данных. Физическая среда. Технологии Fast Ethernet, Gigabit Ethernet, 10G Ethernet.
6	Канальный уровень модели OSI. Коммутаторы	Подуровни канального уровня. MAC-адреса. Протокол ARP. Разделяемая среда, методы доступа. Неразделяемая среда. Беспроводные технологии. Принципы работы коммутатора. Алгоритм покрывающего дерева. Виртуальные сети (VLAN). Иерархическая сетевая модель.
7	Адресация в сетях IP	Типы IPv4-адресов. Формат IP-адреса. Классовая адресация. Бесклассовая адресация. Маска сети. Распределение адресов. Особые IP-адреса. Технология NAT. Адреса IPv6.
8	Транспортный и сетевой уровни модели OSI. Маршрутизация	Порты. Протокол UDP. Стек протоколов TCP/IP. Форматы пакетов TCP и IP. Протокол ICMP. Протокол IPv6. Сравнение и применение протоколов. Задачи, решаемые маршрутизатором. Таблица маршрутизации. Статическая маршрутизация. Виды протоколов динамической маршрутизации. Дистанционно-векторные протоколы: RIPv1 и RIPv2. Протоколы состояния каналов связи: OSPF.
9	Верхние уровни модели OSI	Клиент-серверная модель и одноранговые сети. Протокол Telnet. Система доменных имен. Протокол DHCP. Протокол HTTP. Электронная почта.
10	Беспроводные сети	Распространение электромагнитных волн. Лицензирование частот. Технология широкополосного сигнала. Физические уровни стандарта 802.11. Технология Bluetooth. Безопасность беспроводных сетей.
11	Стандарты информационной безопасности	Стандарты информационной безопасности. Роль стандартов информационной безопасности.

		Международный стандарт ISO 15408. Стандарты для беспроводных сетей. Стандарты информационной безопасности в Интернете.
12	Обнаружение компьютерных атак	Понятие и классификация атак на компьютерные сети. Основные типы сетевых атак. Средства реализации атак. Механизмы типовых атак, основанных на уязвимостях сетевых протоколов. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий. Технологии обнаружения компьютерных атак и их возможности. Прямые и косвенные признаки атак. Методы обнаружения атак. Сигнатурный анализ и обнаружение аномалий. Классификация систем обнаружения атак (СОА). Сетевые и узловые СОА. Требования, предъявляемые к СОА. Стандартизация в области обнаружения атак. Архитектура СОА. Типовая архитектура СОА в составе сенсора, модуля управления, анализатора, набора протоколов взаимодействия и средства реагирования. Эксплуатация СОА. Варианты размещения СОА. Размещение сенсоров СОА. Реагирование на инциденты. Проблемы, связанные с СОА.
13	Технология межсетевого экранирования	Стратегии и средства межсетевого экранирования. Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов. Требования руководящих документов ФСТЭК России к межсетевым экранам. Обзор документов RFC, регламентирующих использование межсетевых экранов. Типы межсетевых экранов. Схемы межсетевого экранирования. Фильтрация пакетов. Критерии и правила фильтрации. Реализация пакетных фильтров. Понятие демилитаризованной зоны. Укрепленный компьютер бастионного типа. Организация узлов для отвлечения внимания злоумышленника. Особенности фильтрации различных типов трафика. Пакетный фильтр на базе ОС Windows. Служба RRAS. Программа управления службой RRAS. Шлюзы прикладного уровня. Сервер SQUID, принципы работы, варианты конфигурации. Контроль HTTP-трафика и электронной почты. Написание правил фильтрации, возможности по анализу содержимого.
14	Организация виртуальных частных сетей	Задачи, решаемые VPN. Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне. Организация VPN средствами протокола PPTP. Установка и настройка VPN. Анализ защищенности передаваемой информации. Защита данных на сетевом уровне. Протокол SKIP. Протокол IPSec. Организация VPN средствами СЗИ «VipNet». Использование протокола IPSec для защиты сетей. Шифрование трафика с использованием протокола IPSec. Настройка политики межсетевого экранирования с использованием протокола IPSec. Организация VPN средствами СЗИ «StrongNet». Описание системы. Генерация и распространение ключевой информации. Настройка СЗИ «StrongNet». Установка защищенного соединения. Защита на транспортном уровне. Организация VPN средствами протокола SSL в Windows Server 2003. Генерация сертификата открытого ключа для web-сервера. Настройка SSL-соединения. Организация VPN прикладного уровня средствами протокола S/MIME и СКЗИ КриптоПро CSP. Защищенный обмен электронной почтой.
15	Технологии защищенной обработки информации	Применение технологии терминального доступа. Общие сведения о технологии терминального доступа.

		Обеспечение безопасности сервера ОС Windows Server 2003. Настройка сервера MSTS. Настройка протокола RDP. Службы каталогов. Общие сведения о службах каталогов. Структура каталога LDAP. Система единого входа в сеть на основе протокола Kerberos. Создание единого пространства безопасности на базе Active Directory.
16	Аудит информационной безопасности в компьютерных сетях	Цели и задачи проведения аудита безопасности. Этапы и методы проведения, результаты работ. Нормативно-правовые и организационные основы проведения аудита безопасности компьютерных систем. Международные, государственные и ведомственные стандарты. Определение структуры информационно-телекоммуникационных сетей. Программные средства анализа топологии вычислительной сети. Определение маршрутов прохождения сетевых пакетов. Обнаружение объектов сети. Построение схемы сети. Выявление телекоммуникационного оборудования. Выявление и построение схемы информационных потоков защищаемой информации. Сетевой мониторинг на основе использования механизма WMI и протоколов ICMP, SNMP и CDP. Применение систем автоматизированного построения схемы сети. Средства и методы выявления уязвимостей в программном обеспечении узлов компьютерной сети. Цели и принципы зондирования узлов сети. Использование коммерческих и свободно распространяемых средств аудита безопасности компьютерных систем. Особенности средств активного аудита. Применение средств анализа защищенности серверов приложений. Применение средств автоматизации комплексного аудита информационной безопасности. Структура и функции комплексных экспертных систем аудита безопасности. Учет структуры аппаратно-программных средств объекта информатизации. Ранжирование обнаруженных уязвимостей по степени воздействия на защищаемую информацию. Описание выявленных уязвимостей и определение мер защиты, их устраняющих. Формирование выводов и рекомендаций по устранению обнаруженных недостатков.

13.2. Разделы дисциплины и виды занятий:

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)				
		Лекции	Лабораторные	Самостоятельная работа	Контроль	Всего
1	Основные понятия компьютерных сетей. Определение локальных сетей и их топология	2	2	3	0	7
2	Типы линий связи локальных сетей. Подключение линий связи и коды передачи информации	2	4	4	0	10
3	Пакеты, протоколы. Методы управления обменом	2	2	4	0	8
4	Сетевая модель OSI	2	4	4	0	10

5	Физический уровень модели OSI. Технология Ethernet	4	2	4	0	10
6	Канальный уровень модели OSI. Коммутаторы	4	4	3	0	11
7	Адресация в сетях IP	4	2	4	0	10
8	Транспортный и сетевой уровни модели OSI. Маршрутизация	6	4	4	4	14
9	Верхние уровни модели OSI	4	2	2	4	8
10	Беспроводные сети	4	2	2	4	8
11	Стандарты информационной безопасности	2	4	4	4	10
12	Обнаружение компьютерных атак	8	4	4	4	16
13	Технология межсетевого экранирования	6	4	6	4	16
14	Организация виртуальных частных сетей	6	4	6	4	16
15	Технологии защищенной обработки информации	6	2	4	4	12
16	Аудит информационной безопасности в компьютерных сетях	6	4	4	4	14
	Итого	68	50	62	36	216

14. Методические указания для обучающихся по освоению дисциплины

(рекомендации обучающимся по освоению дисциплины: работа с конспектами лекций, презентационным материалом, выполнение практических заданий, тестов, заданий текущей аттестации и т.д.)

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины *(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)*

а) основная литература:

№ п/п	Источник
1	*Таненбаум, Эндрю. Компьютерные сети = Computer Networks / Э. Таненбаум ; [пер. с англ. В. Шрага] .— 4-е изд. — СПб. [и др.] : Питер, 2009 .— 991 с. : ил., табл. — (Классика Computer Science) .— Библиогр.: с.952-970 .— Алф. указ.: с.971-991 .— ISBN 978-5-318-00492-6.*
2	*Иванов, Михаил Александрович. Криптографические методы защиты информации в компьютерных системах и сетях / Иванов М. А. — М. : Кудиц-Образ, 2001 .— 363 с. : ил.*

б) дополнительная литература:

№ п/п	Источник
3	*Таненбаум, Эндрю. Компьютерные сети / Э. Таненбаум .— 4-е изд. — СПб. : Питер, 2005 .— 991 с. : ил., табл. — (Классика Computer Science) .— Парал. тит. л. англ. — ISBN 5-318-00492-X.*
4	*Гайдамакин, Н.А. Разграничение доступа к информации в компьютерных системах / Н.А. Гайдамакин .— Екатеринбург : Изд-во Уральского ун-та, 2003 .— 327 с. : ил .— Библиогр.:с.317-322 .— Алф.-предм. указ.: с.306-316 .— ISBN 5-86037-024-5.*
5	*Голуб, Владимир Александрович. Информационная безопасность телекоммуникационных систем : Учебное пособие .— Воронеж : Студия ИАН, 2002 .— 157,[1] с. — ISBN 5-86026-020-2 : 37.00 .— <URL:http://www.lib.vsu.ru/elib/books/b102829.djvu>.*

в) информационные электронно-образовательные ресурсы**:**

№ п/п	Источник
1	*www.fstec.ru, www.securitylab.ru , www.cyberpol.ru , www.azi.ru , www.infotecs.ru , www.infosec.ru , www.infoforum.ru , www.cnews.ru , www.brighttalk.com , www.coresecurity.com .*

16. Перечень учебно-методического обеспечения для самостоятельной работы *(учебно-методические рекомендации, пособия, задачники, методические указания по выполнению практических (контрольных) работ и др.)*

№ п/п	Источник
5	*Скоромников, Кир Серафимович. Компьютерное право Российской Федерации : Учебник / К.С.Скоромников;Междунар.независим. эколого-политол.ун-т .— М. : Изд-во МНЭПУ, 2000 .— 220,[1] с. — ISBN 5-7383-0105-6.*
6	*Велпури, Рама. Oracle8i : Резервное копирование и восстановление / Р. Велпури, А. Адколи ; Пер.с англ. И. Афанасьева; Науч. ред. А. Головко; Авт. предислов. Я. Текер .— М. : Лори, 2002 .— 572 с. : ил .— Парал. тит. л. англ. — ISBN 5-85582-166-8.*
7	*Гайдамакин, Н.А. Разграничение доступа к информации в компьютерных системах / Н.А. Гайдамакин .— Екатеринбург : Изд-во Уральского ун-та, 2003 .— 327 с. : ил .— Библиогр.:с.317-322 .— Алф.-предм. указ.: с.306-316 .— ISBN 5-86037-024-5.*
8	*Голуб, Владимир Александрович. Информационная безопасность телекоммуникационных систем : Учебное пособие .— Воронеж : Студия ИАН, 2002 .— 157,[1] с. — ISBN 5-86026-020-2 : 37.00 .— <URL:http://www.lib.vsu.ru/elib/books/b102829.djvu>.*

17. Информационные технологии, используемые для реализации учебной дисциплины, включая программное обеспечение и информационно-справочные системы (при необходимости)

№ п/п	Источник
1	*www.fstec.ru, www.securitylab.ru , www.cyberpol.ru , www.azi.ru , www.infotecs.ru , www.infosec.ru , www.infoforum.ru , www.cnews.ru , www.brighttalk.com , www.coresecurity.com .*

18. Материально-техническое обеспечение дисциплины:

(при использовании лабораторного оборудования указывать полный перечень, при большом количестве оборудования можно вынести данный раздел в приложение к рабочей программе)

Лекционная аудитория (доска, мел, маркеры), Компьютерный класс (14-15 компьютеров + программное обеспечение) мультимедийный проектор.

19.1. Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

Код и содержание компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков)	Этапы формирования компетенции (разделы (темы) дисциплины или модуля и их наименование)	ФОС* (средства оценивания)
ПК-9 способность выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах	знать: как выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах	Разделы 1-4: 1. Основные понятия компьютерных сетей. Определение локальных сетей и их топология 2. Типы линий связи локальных сетей. Подключение линий связи и коды передачи информации 3. Пакеты, протоколы. Методы управления обменом 4. Сетевая модель OSI	Лабораторные работы и контрольная работа
	уметь: выявлять основные угрозы безопасности информации, строить и	Разделы 5-6: 5. Организационные мероприятия, направленные на	Лабораторные работы и контрольная работа

	исследовать модели нарушителя в компьютерных системах	защиту информации. 6. Программно-аппаратные средства защиты информации	
	владеть (иметь навык(и)): способностью выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах		
ОПК-7 способность применять методы и средства обеспечения информационной безопасности специальных ИАС.	знать: сущность и понятие информации, информационной безопасности и характеристику ее составляющих; место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России; основные свойства информации (ценность, целостность, конфиденциальность, доступность); задачи информационной безопасности; источники и классификацию угроз информационной безопасности, каналы несанкционированного доступа к информации, основные угрозы доступности, целостности и конфиденциальности	Разделы 7-13: 7. Физический уровень модели OSI. Технология Ethernet 8. Канальный уровень модели OSI. Коммутаторы 9.Адресация в сетях IP 10.Транспортный и сетевой уровни модели OSI. Маршрутизация 11. Верхние уровни модели OSI 12. Беспроводные сети 13. Стандарты информационной безопасности	Лабораторные работы и контрольная работа

	информации; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; уровни формирования режима информационной безопасности; правовые основы информационной безопасности; цели и задачи организационно-административного уровня обеспечения информационной безопасности; технические средства обеспечения информационной безопасности; программно-аппаратные средства обеспечения информационной безопасности; основные методы криптографической защиты информации; методы защиты информации в вычислительных сетях; принципы функционирования компьютерных вирусов и методы борьбы с ними;		
	уметь: использовать полученные знания для организации безопасной работы персональных компьютеров; выявлять угрозы информационной безопасности, определять источники этих угроз, их способы реализации и цели; классифицировать защищаемую		Лабораторные работы и контрольная работа

	информацию по видам тайны и степеням конфиденциальности; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; правомерно использовать организационные, технические и программно-аппаратные средства защиты информации; защищать ресурсы персональных компьютеров и сетуй на их основе от компьютерных вирусов и их вредного воздействия; оценить защищенность информационных систем;		
	владеть (иметь навык(и)): профессиональной терминологией в области информационной безопасности; навыками работы со специальной литературой; навыками работы со специализированным программно-аппаратным обеспечением компьютерной безопасности.		
ПК-15 способность эксплуатировать специальные ИАС и средства обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстанавливать их	знать: специальные ИАС и средства обеспечения их информационной безопасности на всех этапах жизненного цикла	14. Обнаружение компьютерных атак 15. Технология межсетевого экранирования 16. Организация виртуальных частных сетей. Технологии защищенной обработки	Лабораторные работы и контрольная работа

работоспособность при внештатных ситуациях		информации	
	уметь: эксплуатировать специальные ИАС и средства обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстанавливать их работоспособность при внештатных ситуациях		
	владеть: способностью эксплуатировать специальные ИАС и средства обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстанавливать их работоспособность при внештатных ситуациях		
Промежуточная аттестация			Комплект КИМ

19.2 Описание критериев и шкалы оценивания компетенций (результатов обучения) при промежуточной аттестации

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в форме лабораторных работ и контрольной работы.

При оценивании используется следующая шкала:

5 баллов ставится, если обучающийся демонстрирует полное соответствие знаний, умений, навыков приведенным в таблицах показателям, свободно оперирует приобретенными знаниями, умениями, применяет их при решении практических задач;

4 балла ставится, если обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач;

3 балла ставится, если обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач;

2 балла ставится, если обучающийся демонстрирует явное несоответствие знаний, умений, навыков приведенным в таблицах показателям.

При сдаче экзамена

оценка «отлично» - 5 баллов

оценка «хорошо» - 4 балла

оценка «удовлетворительно» - 3 балла

оценка «неудовлетворительно» - 2 балла.

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся в полной мере владеет понятийным аппаратом в области программирования и технологии работы на ЭВМ, способен иллюстрировать ответ примерами, фактами, применять теоретические знания для решения практических задач программирования, СУБД и сетевых технологий.	*Повышенный уровень*	*Отлично*
У обучающегося сформированы знания, умения и навыки программирования и технологии работы на ЭВМ; он способен иллюстрировать ответ примерами, фактами, применять теоретические знания для решения практических задач; но допускает отдельные несущественные пробелы в своих	*Базовый уровень*	*Хорошо*

знаниях, допускает ошибки при выполнении практических задач.		
У обучающегося сформированы неполные знания, умения и навыки; он допускает отдельные существенные пробелы в своих знаниях, допускает существенные ошибки при выполнении практических задач.	*Пороговый уровень*	*Удовлетвори-тельно*
Сформированы лишь фрагментарные знания, умения и навыки или знания, умения и навыки отсутствуют	*–*	*Неудовлетвор и-тельно*

19.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы

19.3.1 Перечень вопросов к экзамену 1:
Примерный перечень вопросов к экзамену

1. Правовое регулирование в области безопасности информации: законодательная база информатизации общества; структура государственных органов, обеспечивающих безопасность информационных технологий.
2. Информационная безопасность. Основные определения.
3. Угрозы информационной безопасности.
4. Модель системы зашиты.
5. Организационные меры и меры обеспечения физической безопасности.
6. Идентификация и аутентификация. Методы аутентификации.
7. Особенности парольных систем аутентификации: рекомендации по практической реализации парольных систем, оценка стойкости парольных систем, методы хранения паролей.
8. Методы разграничения доступа. Криптографические методы обеспечения конфиденциальности информации.
9. Методы зашиты внешнего периметра.
10. Системы обнаружения вторжений (Intrusion Detection System, EDS).
11. Протоколирование и аудит.
12. Построение систем защиты от угроз нарушения целостности: типовая структура такой системы.
13. Криптографические методы обеспечения целостности информации: реализация механизма цифровой подписи, криптографические хэш-функции и ее преимущества, коды проверки подлинности.
14. Структура системы защиты от угроз нарушения доступности: поясните основные составляющие.

15. Формальные модели управления доступом: модель Харрисона-Руззо-Ульмана, модель Беллл-ЛаПалулы.

16. Формальные модели целостности: модель Кларка-Вилсона, модель Биба.

17. Основные положения ISO/IEC 15408. Критерии оценки безопасности информационных технологий. Понятия безопасности и их взаимосвязь в соответствии с ГОСТ Р ИСО/МЭК 15408-2002. Структура профиля защиты в соответствии с ГОСТ Р ИСО/МЭК 15408-2002.

18 Основные положения ГОСТ Р ИСО/МЭК 17799:2005 "Информационная технология. Практические правила управления информационной безопасностью".

19 Основные положения ГОСТ Р ИСО/МЭК 27001-2006 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования". Этапы построения и использования СМИБ.

20 Обобщенная схема построения комплексной защиты компьютерной сети предприятия на примере модели Lifecycle Security.

21 Технология функционирования VPN. Типы виртуальных частных сетей, преимущества и недостатки.

22 Методика анализа рисков в сфере информационной безопасности CRAMM.

23 Методика анализа рисков в сфере информационной безопасности FRAP.

24 Методика анализа рисков в сфере информационной безопасности OCTAVE.

25 Методика анализа рисков в сфере информационной безопасности RiskWatch.

26 Проведение оценки рисков в соответствии с методикой Microsoft.

27 Опишите суть протокола системы централизованной аутентификации и распределе-ния ключей симметричного шифрования Kerberos Протоколы и механизмы обеспечения информационной безопасности Kerberos, S/MIME, IPSec, AH, ESP, IPSec, NAT. Опишите их назначение и область применения.

Пример лабораторного задания (вариант задания)

Лабораторная работа № ___

по дисциплине «Основы информационной безопасности»

Тема: «**Шифрование с открытым ключом методом укладки рюкзака**»

Задание. Выберите текст (не менее 60 символов) для шифрования методом укладки рюкзака. Сформируйте закрытую и открытую части ключа. При этом учтите требования, предъявляемые к выбору ключа с целью повышения криптостойкости. Зашифруйте выбранный текст. Сформируйте шифрграмму. Обменяйтесь шифрграммами. Расшифруйте полученный шифртекст. Предполагается, что Вы знаете закрытую и открытую части ключа. Подготовьте отчет.

Вопросы

1. Какие криптосистемы относятся к системам шифрования с открытым ключом? В чем их особенность?
2. Сформулируйте математические основы шифрования с открытым ключом
3. Сформулируйте математические основы шифрования методом укладки рюкзака.

По результатам выполнения заданий подготовьте отчет.

Отчет по лабораторной работе № должен содержать:

1) Титульный лист.
2) Выбранный текст для шифрования.
3) Пояснения по выбору ключа с поверкой требований, предъявляемых к выбору ключа.
4) Пояснения по шифрованию и полученный шифртекст.
5) Шифрграмму, подготовленную Вами, с указанием открытой части ключа.
6) Шифрграмму, полученную Вами при обмене.
7) Пояснения по расшифрованию и полученный открытый текст.
8) Ответы на вопросы.
9) Ваши выводы.

Пример контрольного задания (вариант задания)

Контрольная работа
по дисциплине «Основы информационной безопасности»
Вариант №___

В результате шифрования методом Вижинера был получен следующий шифртекст: «СПЦСЗЗЮУГИВЕБЬБТЖЩИОБ». Прочитайте этот шифртекст, если известно, что шифрующая последовательность содержит только символы А, Б и В.

19.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах: устного опроса (индивидуальный опрос на коллоквиуме); письменных работ (контрольные работы). Критерии оценивания приведены выше.

Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся по программам высшего образования.

Контрольно-измерительные материалы промежуточной аттестации включают в себя теоретические вопросы, позволяющие оценить уровень полученных знаний, или практические задания, позволяющие оценить степень сформированности умений, навыков и опыт деятельности.

При оценивании используются количественные шкалы оценок. Критерии оценивания приведены выше.