МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Набережночелнинский институт (филиал) федерального государственного автономного образовательного учреждения высшего образования

«Казанский (Приволжский) федеральный университет»

ИНЖЕНЕРНО-ЭКОНОМИЧЕСКИЙ КОЛЛЕДЖ

УТВЕРЖДАЮ
Директор
_____Т.И. Бычкова
«_01___» _июня____2017 г.

ПРОГРАММА МЕЖДИСЦИПЛИНАРНОГО КУРСА
МДК.03.02 Безопасность функционирования информационных систем

Специальность: 09.02.02 «Компьютерные сети»
Квалификация выпускника: техник по компьютерным сетям
Форма обучения: очная
на базе основного общего образования
Язык обучения: русский
Автор: Абросимова Е.В.
Рецензент: Ахметов М.Р.

СОГЛАСОВАНО: Председатель ПЦК «Цикл информатики и информационных технологий»:
_____Рязанова А.Н.

Протокол заседания ПЦК № 12 от « 24 » мая 2017г.

Учебно-методическая комиссия инженерно-экономического колледжа

Протокол заседания УМК № 14 от « 30 » мая 2017г.

г. Набережные Челны, 2017

1. Цели освоения междисциплинарного курса

Программа МДК.03.02 «Безопасность функционирования информационных систем» является частью основной образовательной программы в соответствии с ФГОС по специальности 09.02.02 «Компьютерные сети».

Цель изучения МДК.03.02 «Безопасность функционирования информационных систем» – является формирование знаний об объектах и задачах защиты компьютерных систем, способах и средствах нарушения информационной безопасности, о принципах и подходах к решению задач защиты информации; а также формирование умений по применению современных технологий, выбора средств и инструментов защиты информации для построения современных защищенных информационных систем в соответствии с действующим законодательством.

Задачи изучения междисциплинарного курса:

- изучение основ проектирования и эксплуатации защищенных информационных систем;
- изучение принципов администрирования сетевых служб;
- изучение способов обеспечения работоспособности и доступности серверов;
- изучение клиентской части программного обеспечения.

2. Место междисциплинарного курса в структуре ППССЗ

МДК.03.02 «Безопасность функционирования информационных систем» входит в профессиональный модуль ПМ.03«Эксплуатация объектов сетевой инфраструктуры».

Осваивается на четвертом курсе (8 семестр).

3. Компетенции обучающегося, формируемые в результате освоения междисциплинарного курса

В результате освоения междисциплинарного курса обучающийся должен *знать:*

- основные понятия информационных систем, жизненный цикл, проблемы обеспечения технологической безопасности информационных систем, требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования, оперативные методы повышения безопасности функционирования программных средств и баз данных;
- основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем
- средства защиты информации в автоматизированных системах обработки данных;
- компьютерные вирусы и антивирусные программы;
- политику информационной безопасности;
- стандарты информационной безопасности.

В результате освоения междисциплинарного курса обучающийся должен *уметь:*

- устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту
- организовывать защиту информации в автоматизированных системах обработки данных;
- использовать антивирусные программы.

В результате освоения междисциплинарного курса обучающийся должен *иметь практический опыт*:

- обслуживания сетевой инфраструктуры, восстановления работоспособности сети после сбоя;
- удаленного администрирования и восстановления работоспособности сетевой инфраструктуры;
- организации бесперебойной работы системы по резервному копированию и восстановлению информации;
- поддержки пользователей сети, настройки аппаратного и программного обеспечения сетевой инфраструктуры.

В результате освоения дисциплины формируются компетенции:

Шифр компетенции	**Расшифровка приобретаемой компетенции**
ОК 1	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес
ОК 2	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество
ОК 3	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность
ОК 4	Осуществлять поиск и использование информации, необходимой для эффективного выполнения
ОК 5	Использовать информационно-коммуникационные технологии в профессиональной деятельности
ОК 6	Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями
ОК 7	Брать на себя ответственность за работу членов команды (подчиненных) за результат выполнения заданий
ОК 8	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации
ОК 9	Ориентироваться в условиях частой смены технологий в профессиональной деятельности
ПК 3.1	Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей.
ПК 3.2	Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях
ПК 3.3	Эксплуатация сетевых конфигураций.
ПК 3.4	Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации
ПК 3.5	Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль поступившего из ремонта оборудования
ПК 3.6	Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.

4. Структура и содержание междисциплинарного курса

4.1. Распределение трудоёмкости междисциплинарного курса (в часах) по видам нагрузки обучающегося и по разделам междисциплинарного курса

Общая трудоемкость междисциплинарного курса составляет 238 часов.

Форма промежуточной аттестации по междисциплинарному курсу: экзамен в 8 семестре.

Разделы и темы междисциплинарного курса		Семестр	Неделя	Виды и часы аудиторной работы, их трудоемкость (в часах)			Самостоятельная работа	Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы		
Раздел 1	**Основы проектирования и эксплуатации защищенных информационных систем**			**32**	**38**	**0**	**36**	
Тема 1.1	Основные понятия и определения	8	1	4	4	0	6	Устный опрос Практическая работа 1
Тема 1.2	Проблема обеспечения безопасности в информационных системах	8	1	4	6	0	6	Устный опрос Практическая работа 2
Тема 1.3	Специфика эксплуатации защищенных ИС	8	2	4	6	0	6	Устный опрос Практическая работа 3
Тема 1.4	Концепция проектирования системы защиты ИС	8	3-5	8	6	0	6	Устный опрос Практическая работа 4
Тема 1.5	Общий состав работ на этапе эксплуатации	8	5	6	8	0	6	Устный опрос Практическая работа 5

	IT-систем							
Тема 1.6	Требования по защите информационных систем, устанавливаемые законодательством РФ	8	5	6	8	0	6	Устный опрос Практическая работа 6 *Тест 1
Раздел 2	**Администрирование сетевых служб**			**24**	**26**	**0**	**28**	
Тема 2.1	Сканеры безопасности.	8	6	4	4	0	6	Устный опрос Практическая работа 7
Тема 2.2	Межсетевые экраны	8	6	6	6	0	4	Устный опрос Практическая работа 8
Тема 2.3	Виртуальные частные сети	8	7	4	6	0	6	Устный опрос Практическая работа 9
Тема 2.4	Системы обнаружения вторжений	8	7	4	6	0	6	Устный опрос Практическая работа 10
Тема 2.5	Защита беспроводных сетей	8	8	6	4	0	6	Устный опрос Практическая работа 11 *Тест 2
Раздел 3	**Внедрение инфраструктуры открытых ключей**			**8**	**4**		**6**	
Тема 3.1	Развертывание инфраструктуры открытых ключей	8	8	8	4	0	6	Устный опрос Практическая работа 12 *Тест 3
Раздел 4	**Обеспечение работоспособности и доступности серверов**			**16**	**12**	**0**	**8**	
Тема 4.1	Организация резервного копирования на серверах Windows.	8	9	8	6	0	4	Устный опрос Практическая работа 13,14
Тема 4.2	RAID и зеркалирование	8	10	8	6	0	4	Устный опрос Практическая работа 15,16
	Всего			**80**	**80**	**0**	**78**	

***** - контрольные точки

4.2. Содержание междисциплинарного курса

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения
1	**2**	**3**	
Раздел 1. Основы проектирования и эксплуатации защищенных информационных систем		**106**	
Тема 1.1. Основные понятия и определения	**Содержание учебного материала**	2	
	1 **Основные понятия информационных систем:** информация, информационные процессы, поиск информации, хранение информации, сбор. Передача информации, обработка, использование.		2
	2 **Информационные ресурсы и технологии:** информационные ресурсы, информационные технологии.	2(2)	
	Практическая работа 1. Программирование арифметических алгоритмов Цели и задачи криптографии. Исследование и разработка основных методов симметричных криптосистем.	4(4)	
	Самостоятельная работа 1.Работа с конспектом лекции 2.Конспектирование учебной литературы по теме 1.1	6(8)	
Тема 1.2. Проблема обеспечения безопасности в информационных системах.	**Содержание учебного материала**	2(14)	
	1 **Свойства информации:** доступность целостность конфиденциальность		2
	2 **Классификации угроз:** Классификация угроз по используемым средствам. Классификация по характеру действий, используемых в атаке. Классификация по характеру уязвимостей. Классификация типовых удаленных атак по виду воздействия.	2(16)	

	Практическая работа 2. Программирование арифметических алгоритмов 1.Шифрование методом замены. 2.Шифр Цезаря.		6(18)	
	Самостоятельная работа 1. Работа с конспектом лекции 2.Конспектирование учебной литературы по теме 1.2		6(24)	
Тема 1.3. Специфика эксплуатации защищенных ИС	**Содержание учебного материала**		2(30)	
	1	Основная особенность эксплуатации средств и систем информационной безопасности.		2
	2	Возрастание сложности ИС, новые угрозы безопасности, особенности ИС.	2(32)	
	Практическая работа 3. Программирование арифметических алгоритмов 1.Изучение подстановочного шифра. 2.Шифр Виженера (Vigenere) и его варианты		6(34)	
	Самостоятельная работа 1. Работа с конспектом лекции 2.Конспектирование учебной литературы по теме 1.3		6(40)	
Тема 1.4. Концепция проектирования системы защиты ИС	**Содержание учебного материала**		2(46)	
	1	Анализ бизнес-требований к защите информации в ИС, влияние общих бизнес-факторов на проект защиты. Снижение влияния несовместимости систем на их защиту.		2
	2	Угрозы безопасности ИС, возникающие из-за проблем с сопровождением. Разработка концептуального плана защиты. Принципы проектирования защиты информации.	2(48)	
	3	Рекомендации по проектированию защищенных элементов ИС. Укрепление защиты внутренней сети при помощи сегментирования.	2(50)	
	4	Планирование процедуры восстановления. Анализ технических ограничений, правила интеграции. Анализ ограничений по совместимости.	2(52)	

	Практическая работа 4. Программирование арифметических алгоритмов 1.Изучение метода частотного криптоанализа. 2.Частотный анализ.		6(54)	
	Самостоятельная работа 1. Работа с конспектом лекции 2.Конспектирование учебной литературы по теме 1.4		6(60)	
Тема 1.5 Общий состав работ на этапе эксплуатации IT-систем	**Содержание учебного материала**		2(66)	
	1	Понятие грамотной эксплуатации системы. Мониторинг в режиме реального времени и анализ происходящих в ИС событий.		2
	2	Контроль безопасности системы. Преодоление нештатных ситуаций.	2(68)	
	3	Техническая поддержка средств и систем защиты. Анализ и контроль защищенности ресурсов.	2(70)	
	Практическая работа 5. Программирование арифметических алгоритмов 1. Обычная перестановка. 2. Усложненная перестановка. 3. Шифры двойной перестановки. 4. Шифрование с помощью магического квадрата.		8(72)	
	Самостоятельная работа 1. Работа с конспектом лекции 2.Конспектирование учебной литературы по теме 1.5		6(80)	
Тема 1.6 Требования по защите информационных систем, устанавливаемые законодательством РФ	**Содержание учебного материала**		2(86)	
	1	Требования по защите информации от НСД в соответствии с Руководящими Документами России. Понятие класса защищенности, групп автоматизированных систем.		2
	2	Требования к подсистемам защиты для каждого класса защищенности.	2(88)	
	3	Основные меры защиты информации в автоматизированных системах. Основные положения и требования для обеспечения защиты информации в процессе эксплуатации.	2(90)	

	Практическая работа 6. Программирование алгебраических алгоритмов 1.Одноалфавитная замена. 2.Моноалфавитная замена.		8(92)	
	Самостоятельная работа 1. Работа с конспектом лекции 2.Конспектирование учебной литературы по теме 1.6 3.Подготовка к тесту 1		6(100)	
Раздел 2. Администрирование сетевых служб			**80**	
Тема 2.1. Сканеры безопасности	**Содержание учебного материала**		2(106)	
	1	Понятия уязвимости, угрозы. Определение сканера безопасности. Принципы работы сканера безопасности.		2
	2	Классы сканеров безопасности и их краткая характеристика. Недостатки сканеров безопасности.	2(102)	
	Практическая работа 7. Программирование алгебраических алгоритмов 1.Шифр Гронсфельда.		4(104)	
	Самостоятельная работа 1. Работа с конспектом лекции 2.Конспектирование учебной литературы по теме 2.1		6(108)	
Тема 2.2. Межсетевые экраны	**Содержание учебного материала**		2(114)	
	1	Риски, связанные с подключением компьютера к глобальной сети		2
	2	Интернет, понятие межсетевого экрана, виды межсетевых экранов	2(116)	
	3	Кратная характеристика, правила функционирования межсетевых экранов.	2(118)	
	Практическая работа 8. Программирование алгоритмов криптосистем с открытым ключом		6(120)	

	1.Алгоритм шифрации двойным квадратом. Шифр Enigma. 2.Алгоритм шифрования DES.		
	Самостоятельная работа 1. Работа с конспектом лекции 2.Конспектирование учебной литературы по теме 2.2	4(126)	
Тема 2.3. Виртуальные частные сети	**Содержание учебного материала**	2(130)	
	1 Понятие виртуальных частных сетей, криптозащищенных туннелей, инициатора и терминатора туннеля.		2
	2 Протоколы поддержки виртуальных частных сетей.	2(132)	
	Практическая работа 9. Программирование алгоритмов криптосистем с открытым ключом 1.Алгоритм шифрования ГОСТ 28147-89. 2.Алгоритм шифрования RSA.	6(134)	
	Самостоятельная работа 1. Работа с конспектом лекции 2.Конспектирование учебной литературы по теме 2.3	6(142)	
Тема 2.4. Системы обнаружения вторжений	**Содержание учебного материала**	2(148)	
	1 Понятие системы обнаружения вторжений. Основные виды систем обнаружения вторжений. Достоинства и недостатки.		2
	2 Понятие сниффинга. Снифферы, их легальное и нелегальное применение.	2(150)	
	Практическая работа 10. Программирование алгоритмов криптосистем с открытым ключом 1.Алгоритм шифрования Эль Гамаля. 2.Задачи и алгоритмы электронной подписи. 3.Задачи распределения ключей.	6(152)	
	Самостоятельная работа 1. Работа с конспектом лекции 2.Конспектирование учебной литературы по теме 2.4	6 (158)	
Тема 2.5. Защита	**Содержание учебного материала**	2(164)	

беспроводных сетей	1	Стандарты и топологии беспроводных сетей. Понятие точки доступа.		2
	2	Защита беспроводных сетей, основные угрозы безопасности беспроводных сетей. Управление беспроводными сетями при помощи групповых политик.	2(166)	
	3	Шифрование трафика беспроводной сети. Методы аутентификации пользователей в беспроводных сетях.	2(168)	
	Практическая работа 11. Защита от закладок при разработке программ (семинар) 1.Почему при эксплуатации компьютерной системы важно знать ее параметры? 2.Какие стандартные средства Windows XP обеспечивают пользователю возможность определения параметров компьютерной системы? 3.Почему обеспечение бесперебойной работы дисковой системы компьютера является одной из основных мер обеспечения информационной безопасности?		4(172)	
	Самостоятельная работа 1. Работа с конспектом лекции 2.Конспектирование учебной литературы по теме 2.5 3. Подготовка к тесту 2		6(176)	
Раздел 3. Внедрение инфраструктуры открытых ключей			**18**	
Тема 3.1 Развертывание инфраструктуры открытых ключей	**Содержание учебного материала**		2(182)	
	1	Предварительный этап — Подготовка принятия решения о развертывании PKI. Оценка готовности к развертыванию. Определение цели развертывания PKI.		2
	2	Определение сферы применения PKI. Выбор приоритетных сервисов безопасности. Анализ данных и приложений Проектирование PKI — Формирование политики PKI. Модель доверия и архитектура PKI.	2(184)	
	3	Политика применения сертификатов. Выбор программного продукта или поставщика услуг PKI. Интеграция PKI с действующими системами и приложениями.	2(186)	

	4	Серверы и криптографическое аппаратное обеспечение. Смарт-карты и считыватели. Физическая среда. Управление и администрирование системы PKI	2(188)	
	Практическая работа 12. Защита от закладок при разработке программ (семинар) 1.Опишите причины нарушений в работе магнитных дисков. 2.Почему необходима процедура очистки диска? 3.Что такое фрагментация файла? Почему она возникает и как влияет на скорость операций чтения информации с диска? 4.Что такое фрагментация файла? В каких случаях рекомендуется выполнить дефрагментацию диска?		4(190)	
	Самостоятельная работа 1. Работа с конспектом лекции 2.Конспектирование учебной литературы по теме 3.1 3. Подготовка к тесту 3		6(194)	
Раздел 4. Обеспечение работоспособности и доступности серверов			**34**	
Тема 4.1. Организация резервного копирования на серверах Windows	**Содержание учебного материала**		2(202)	
	1	Оборудование для архивации.		2
	2	Создание плана резервного копирования	2(204)	
	3	Выбор архивируемых данных	2(206)	
	4	Типы архивации.	2(208)	
	Практическая работа 13. Защита от закладок при разработке программ (семинар) 1.С какой целью выполняется архивация данных компьютера? 2.Что такое дискета аварийного восстановления? Какой программой она создается? 3.Какие вы знаете программы восстановления информации на магнитных дисках? **Практическая работа 14. Профилактика заражения вирусами**		6(210)	

	компьютерных систем (семинар) 1.Что такое компьютерный вирус? Какими свойствами обладают компьютерные вирусы? 2.По каким признакам классифицируют компьютерные вирусы? Перечислите типы вирусов. 3.Какие вирусы называются резидентными и в чем особенность таких вирусов? 4.Каковы отличия вирусов-репликаторов, стелс - вирусов, мутантов и «троянских» программ? 5.Опишите схему функционирования загрузочного вируса. 6.Опишите схему функционирования файлового вируса. 7.Опишите схему функционирования загрузочно-файловых вирусов, особенности.			
	Самостоятельная работа 1. Работа с конспектом лекции 2.Конспектирование учебной литературы по теме 4.1		4(216)	
Тема 4.2. RAID и зеркалирование	**Содержание учебного материала**		2(220)	
	1	Классификация RAID-массивов.		2
	2	Комбинированные уровни RAID.	2(222)	
	3	Программный RAID в Windows	2(224)	
	4	Программный RAID в Linux	2(226)	
	Практическая работа 15. Профилактика заражения вирусами компьютерных систем (семинар) 1.Что такое полиморфный вирус? Почему этот тип вирусов считается наиболее опасным? 2.Каковы причины появления компьютерных вирусов. Приведите примеры широко известных вирусов. 3.Существует ли в мире и в РФ уголовная ответственность за создание и распространение компьютерных вирусов?		6(228)	

	4.Каковы пути проникновения вирусов в компьютер и признаки заражения компьютера вирусом? 5.Каковы способы обнаружения вирусов и антивирусной профилактики? 6.Перечислите основные меры по защите от компьютерных вирусов. 7.Опишите назначение антивирусных программ различных типов. 8.Назовите примеры современных антивирусных программ и опишите их **Практическая работа 16. Виды угроз информационной безопасности Российской Федерации (семинар)** 1.Перечислите виды угроз безопасности информационного общества. 2.В чем заключается угроза раскрытия информации? Какие еще угрозы Вы знаете? 3.Что положено в основу дискреционной модели доступа? 4.Раскройте понятие троянской программы в контексте защиты информации в вычислительной системе.		
	Самостоятельная работа 1. Работа с конспектом лекции 2.Конспектирование учебной литературы по теме 4.2	4(234)	
	Всего:	**238**	

4.3. Структура и содержание самостоятельной работы междисциплинарного курса

№	Раздел междисциплинарного курса	Виды самостоятельной работы	Трудоемкость (в часах)	Формы контроля самостоятельной работы
Раздел 1. Основы проектирования и эксплуатации защищенных информационных систем				
1	Основные понятия и определения	Подготовка к устному опросу	3	Устный опрос
		Конспектирование литературы	3	Проверка конспекта
2	Проблема обеспечения безопасности в информационных системах	Подготовка к устному опросу	3	Устный опрос
		Конспектирование литературы	3	Проверка конспекта
3	Специфика эксплуатации защищенных информационных систем	Подготовка к устному опросу	3	Устный опрос
		Конспектирование литературы	3	Проверка конспекта
4	Концепция проектирования системы защиты информационных систем	Подготовка к устному опросу	3	Устный опрос
		Конспектирование литературы	3	Проверка конспекта
5	Общий состав работ на этапе эксплуатации IT-систем	Подготовка к устному опросу	3	Устный опрос
		Конспектирование литературы	3	Проверка конспекта
6	Требования по защите информационных систем, устанавливаемые законодательством РФ	Подготовка к устному опросу	1,5	Устный опрос
		Конспектирование литературы	1,5	Проверка конспекта
		Подготовка к тестированию по разделу «Основы проектирования и эксплуатации защищенных информационных систем»	3	Тестирование
Раздел 2. Администрирование сетевых служб				
7	Сканеры безопасности.	Подготовка к устному опросу	2	Устный опрос
		Конспектирование литературы	2	Проверка конспекта
8	Межсетевые экраны	Подготовка к устному опросу	2	Устный опрос
		Конспектирование литературы	2	Проверка конспекта
9	Виртуальные частные сети	Подготовка к устному опросу	3	Устный опрос
		Конспектирование литературы	3	Проверка конспекта
10	Системы	Подготовка к устному опросу	3	Устный опрос

	обнаружения вторжений	Конспектирование литературы	3	Проверка конспекта
11	Защита беспроводных сетей	Подготовка к устному опросу	1,5	Устный опрос
		Конспектирование литературы	1,5	Проверка конспекта
		Подготовка к тестированию по разделу «Администрирование сетевых служб»	3	Тестирование
Раздел 3. Внедрение инфраструктуры открытых ключей				
12	Развертывание инфраструктуры открытых ключей	Подготовка к устному опросу	2	Устный опрос
		Конспектирование литературы	2	Проверка конспекта
		Подготовка к тестированию по разделу «Внедрение инфраструктуры открытых ключей»	2	Тестирование
Раздел 4. Обеспечение работоспособности и доступности серверов				
13	Организация резервного копирования на серверах Windows.	Подготовка к устному опросу	2	Устный опрос
		Конспектирование литературы	2	Проверка конспекта
14	RAID и зеркалирование	Подготовка к устному опросу	2	Устный опрос
		Конспектирование литературы	2	Проверка конспекта
ИТОГО			**78**	

5. Образовательные технологии

Практические занятия проводятся с использованием активных методов: работа в малых группах, решение кейсов (анализ реальных проблемных ситуаций, имевших место в соответствующей области профессиональной деятельности, и поиск вариантов лучших решений), проблемное обучение (стимулирование студентов к самостоятельному приобретению знаний, необходимых для решения конкретной проблемы). Самостоятельная работа студента предполагает изучение студентами нового материала до его изучения в ходе аудиторных занятий, выполнение практических заданий. Выполнение заданий требует использования не только учебников и пособий, но и информации, содержащейся в периодических изданиях, Интернете.

На лекциях:

- информационная и презентационная лекция.

На практических занятиях:

- выполнение практических работ в подгруппах для обобщения тематического теоретического материала;

- выполнение самостоятельных работ

Занятия, проводимые в активной и интерактивной формах

Номер темы	Наименование темы	Форма проведения занятия	Объем в часах
Тема 2.1	Сканеры безопасности.	Презентация	4
Тема 2.2	Межсетевые экраны	Презентация	6
Тема 2.3	Виртуальные частные сети	Презентация	4
Тема 3.1	Развертывание инфраструктуры открытых ключей	Мозговой штурм (мозговая атака)	8
Тема 4.1	Организация резервного копирования на серверах Windows.	Действия по алгоритму	8
Всего по дисциплине			**30**

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения междисциплинарного курса и учебно-методическое обеспечение самостоятельной работы обучающихся

Оценочные средства текущего контроля

Тема 1.1. Основные понятия и определения

Устный опрос: Информация, информационные процессы, поиск информации, хранение информации, сбор. Передача информации, обработка, использование. Информационные ресурсы, информационные технологии.

Практическая работа 1. Программирование арифметических алгоритмов

Цели и задачи криптографии. Исследование и разработка основных методов симметричных криптосистем.

Тема 1.2. Проблема обеспечения безопасности в информационных системах.

Устный опрос: Доступность, целостность, конфиденциальность. Классификация угроз по используемым средствам. Классификация по характеру действий, используемых в атаке. Классификация по характеру уязвимостей. Классификация типовых удаленных атак по виду воздействия.

Практическая работа 2. Программирование арифметических алгоритмов

Задания

1. Зашифровать любой текст шифрованием методом замены (Шифр Цезаря).
2. Расшифровать любой другой текст зашифрованный шифром Цезаря.

Тема 1.3. Специфика эксплуатации защищенных информационных систем

Устный опрос: Основная особенность эксплуатации средств и систем информационной безопасности. Возрастание сложности информационных систем, новые угрозы безопасности, особенности информационных систем.

Практическая работа 3. Программирование арифметических алгоритмов

Задания

1. Зашифровать любой текст с помощью подстановочного шифра (Шифр Виженера).
2. Расшифровать любой другой текст зашифрованный шифром Виженера (либо в обратном направлении, либо с помощью простой замены).

Тема 1.4. Концепция проектирования системы защиты информационных систем

Устный опрос: Анализ бизнес-требований к защите информации в информационных системах, влияние общих бизнес-факторов на проект защиты. Снижение влияния несовместимости систем на их защиту. Угрозы безопасности информационных систем, возникающие из-за проблем с сопровождением. Разработка концептуального плана защиты. Принципы проектирования защиты информации. Рекомендации по проектированию защищенных элементов информационных систем. Укрепление защиты внутренней сети при помощи сегментирования. Планирование процедуры восстановления. Анализ технических ограничений, правила интеграции. Анализ ограничений по совместимости.

Практическая работа 4. Программирование арифметических алгоритмов

Задания

1. Зашифровать любой текст с помощью подстановочного шифра (Шифр Виженера).
2. Расшифровать любой другой текст методом частотного анализа.

Тема 1.5. Общий состав работ на этапе эксплуатации IT-систем

Устный опрос: Понятие грамотной эксплуатации системы. Мониторинг в режиме реального времени и анализ происходящих в ИС событий. Контроль безопасности системы. Преодоление нештатных ситуаций. Техническая поддержка средств и систем защиты. Анализ и контроль защищенности ресурсов.

Практическая работа 5. Программирование арифметических алгоритмов

Задания

1. Зашифровать любой текст с помощью шифра простой перестановки.
2. Расшифровать любой другой текст зашифрованный шифром простой перестановки.
3. Зашифровать любой текст с помощью шифра одиночной перестановки по ключу.
3. Расшифровать любой другой текст зашифрованный шифром одиночной перестановки по ключу.
4. Зашифровать любой текст с шифрованием с помощью магического квадрата.

Тема 1.6. Требования по защите информационных систем, устанавливаемые законодательством РФ

Устный опрос: Требования по защите информации от НСД в соответствии с Руководящими Документами России. Понятие класса защищенности, групп автоматизированных систем. Требования к подсистемам защиты для каждого класса защищенности. Основные меры защиты информации в автоматизированных системах. Основные положения и требования для обеспечения защиты информации в процессе эксплуатации.

Практическая работа 6. Программирование алгебраических алгоритмов

Задания

1. Зашифровать любой текст с помощью шифра одноалфавитной замены.
2. Расшифровать любой другой текст зашифрованный шифром одноалфавитной замены.
3. Зашифровать любой текст с помощью шифра многоалфавитной замены.
4. Расшифровать любой другой текст зашифрованный шифром многоалфавитной замены.

Тест 1 по разделу «Основы проектирования и эксплуатации защищенных информационных систем».

Темы: Основные понятия и определения.

Проблема обеспечения безопасности в информационных системах.

Специфика эксплуатации защищенных ИС.

Концепция проектирования системы защиты ИС.

Общий состав работ на этапе эксплуатации IT-систем.

Требования по защите информационных систем, устанавливаемые законодательством РФ.

1. Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это….
    1. **информационная война**
    2. информационное оружие
    3. информационное превосходство

2. Информация не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения в преимущественное положение по сравнению с другими объектами.
    1. служебная информация
    2. коммерческая тайна
    3. банковская тайна
    4. **конфиденциальная информация**

3. Гарантия того, что конкретная информация доступна только тому кругу лиц, для которых она предназначена
    1. **конфиденциальность**
    2. целостность
    3. доступность
    4. аутентичность
    5. аппелеруемость

4. Гарантия того, что АС ведет себя в нормальном и внештатном режиме так, как запланировано
    1. **надежность**
    2. точность
    3. контролируемость
    4. устойчивость
    5. доступность

5. Способность системы к целенаправленному приспособлению при изменении структуры, технологических схем или условий функционирования, которое спасает владельца АС от необходимости принятия кардинальных мер по полной замене средств защиты на новые.
    1. принцип системности
    2. принцип комплексности
    3. принцип непрерывной защиты
    4. принцип разумной достаточности
    5. **принцип гибкости системы**

6. В классификацию вирусов по способу заражения входят
    1. опасные
    2. файловые
    3. **резидентные**
    4. загрузочные
    5. файлово -загрузочные

6. **нерезидентные**

7. Комплекс превентивных мер по защите конфиденциальных данных и информационных процессов на предприятии это…
   1. **комплексное обеспечение ИБ**
   2. безопасность АС
   3. угроза ИБ
   4. атака на АС
   5. политика безопасности

8. Вирусы, не связывающие свои копии с файлами, а создающие свои копии на дисках, не изменяя других файлов, называются:
   1. компаньон - вирусами
   2. **черви**
   3. паразитические
   4. студенческие
   5. призраки
   6. стелс - вирусы
   7. макровирусы

9. К видам системы обнаружения атак относятся :
   1. системы, обнаружения атаки на ОС
   2. системы, обнаружения атаки на конкретные приложения
   3. системы, обнаружения атаки на удаленных БД
   4. **все варианты верны**

10. Автоматизированная система должна обеспечивать
   1. надежность
   2. **доступность**
   3. **целостность**
   4. контролируемость

11. Основными компонентами парольной системы являются
   1. **интерфейс администратора**
   2. хранимая копия пароля
   3. **база данных учетных записей**
   4. все варианты верны

12. Некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации это ….
   1. идентификатор пользователя
   2. **пароль пользователя**
   3. учетная запись пользователя
   4. парольная система

13. К принципам информационной безопасности относятся
   1. скрытость
   2. масштабность
   3. **системность**
   4. **законность**
   5. **открытости алгоритмов**

14. К вирусам изменяющим среду обитания относятся:
   1. черви
   2. студенческие
   3. **полиморфные**
   4. спутники

15. Охрана персональных данных, государственной служебной и других видов информации ограниченного доступа это…

1. **Защита информации**
2. Компьютерная безопасность
3. Защищенность информации
4. Безопасность данных

16. Система физической безопасности включает в себя следующие подсистемы:
    1. **оценка обстановки**
    2. скрытность
    3. **строительные препятствия**
    4. **аварийная и пожарная сигнализация**
17. Какие степени сложности устройства Вам известны
    1. упрощенные
    2. **простые**
    3. **сложные**
    4. оптические
    5. встроенные
18. К механическим системам защиты относятся:
    1. **проволока**
    2. **стена**
    3. сигнализация
    4. **вы**
19. Какие компоненты входят в комплекс защиты охраняемых объектов:
    1. **сигнализация**
    2. **охрана**
    3. **датчики**
    4. **телевизионная система**
20. К выполняемой функции защиты относится:
    1. внешняя защита
    2. внутренняя защита
    3. **все варианты верны**
21. Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных:
    1. Защита информации
    2. **Компьютерная безопасность**
    3. Защищенность информации
    4. Безопасность данных
22. Средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним это:
    1. информационная война
    2. **информационное оружие**
    3. информационное превосходство
23. Информация позволяющая ее обладателю при существующих или возможных обстоятельствах увеличивать доходы, сохранить положение на рынке товаров, работ или услуг это:
    1. государственная тайна
    2. **коммерческая тайна**
    3. банковская тайна
    4. конфиденциальная информация
24. Гарантия того, что при хранении или передаче информации не было произведено несанкционированных изменений:
    1. конфиденциальность
    2. **целостность**

3. доступность
4. аутентичность
5. аппелеруемость

25. Гарантия точного и полного выполнения команд в АС:
1. надежность
2. **точность**
3. контролируемость
4. устойчивость
5. доступность

26. Уровень защиты, при котором затраты, риск, размер возможного ущерба были бы приемлемыми:
1. принцип системности
2. принцип комплексности
3. принцип непрерывности
4. **принцип разумной достаточности**
5. принцип гибкости системы

27. Совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты АС от заданного множества угроз безопасности:
1. Комплексное обеспечение информационной безопасности
2. Безопасность АС
3. Угроза информационной безопасности
4. атака на автоматизированную систему
5. **политика безопасности**

28. Особенностями информационного оружия являются:
1. системность
2. открытость
3. **универсальность**
4. **скрытность**

29. К функциям информационной безопасности относятся:
1. **совершенствование законодательства РФ в сфере обеспечения информационной безопасности**
2. **выявление источников внутренних и внешних угроз**
3. **Страхование информационных ресурсов**
4. **защита государственных информационных ресурсов**
5. **подготовка специалистов по обеспечению информационной безопасности**

30. К типам угроз безопасности парольных систем относятся
1. словарная атака
2. тотальный перебор
3. атака на основе психологии
4. разглашение параметров учетной записи
5. **все варианты ответа верны**

31. К вирусам не изменяющим среду обитания относятся:
1. **черви**
2. студенческие
3. полиморфные
4. **спутники**

32. Хранение паролей может осуществляться
1. **в виде сверток**
2. **в открытом виде**
3. в закрытом виде
4. **в зашифрованном виде**
5. все варианты ответа верны

33. Антивирусная программа принцип работы, которой основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых вирусов называется:

1. ревизором
2. иммунизатором
3. **сканером**
4. доктора и фаги

34. Выбрать недостатки имеющиеся у антивирусной программы ревизор:

1. **неспособность поймать вирус в момент его появления в системе**
2. **небольшая скорость поиска вирусов**
3. **невозможность определить вирус в новых файлах (в электронной почте, на дискете)**

Тема 2.1 Сканеры безопасности

Устный опрос: Понятия уязвимости, угрозы. Определение сканера безопасности. Принципы работы сканера безопасности. Классы сканеров безопасности и их краткая характеристика. Недостатки сканеров безопасности.

Практическая работа 7. Программирование алгебраических алгоритмов

Задания

1. Зашифровать любой текст с помощью шифра Гронсфельда.
2. Расшифровать любой другой текст зашифрованный шифром Гронсфельда.

Тема 2.2 Межсетевые экраны

Устный опрос: Риски, связанные с подключением компьютера к глобальной сети. Интернет, понятие межсетевого экрана, виды межсетевых экранов и их кратная характеристика, правила функционирования межсетевых экранов.

Практическая работа 8. Программирование алгоритмов криптосистем с открытым ключом

Задания

1. Зашифровать любой текст с помощью шифра двойного квадрата.
2. Зашифровать любой текст с помощью шифрования DES.
3. Расшифровать любой другой текст зашифрованный с помощью шифрования DES

Тема 2.3 Виртуальные частные сети

Устный опрос: Понятие виртуальных частных сетей, криптозащищенных туннелей, инициатора и терминатора туннеля. Протоколы поддержки виртуальных частных сетей.

Практическая работа 9. Программирование алгоритмов криптосистем с открытым ключом

Задания

1. Зашифровать любой текст с помощью шифра ГОСТ 28147-89.
2. Зашифровать любой текст с помощью шифра RSA.
3. Расшифровать любой другой текст, зашифрованный с помощью шифра RSA.

Тема 2.4 Системы обнаружения вторжений

Устный опрос: Понятие системы обнаружения вторжений. Основные виды систем обнаружения вторжений. Достоинства и недостатки. Понятие сниффинга. Снифферы, их легальное и нелегальное применение.

Практическая работа 10. Программирование алгоритмов криптосистем с открытым ключом

Задания

1. Зашифровать любой текст с помощью шифра Эль Гамаля.
2. Расшифровать любой другой текст, зашифрованный с помощью шифра Эль Гамаля.
3. Рассмотреть задачи и алгоритмы электронной подписи.
4. Рассмотреть задачи распределения ключей.

Тема 2.5 Защита беспроводных сетей

Устный опрос: Стандарты и топологии беспроводных сетей. Понятие точки доступа. Защита беспроводных сетей, основные угрозы безопасности беспроводных сетей. Управление беспроводными сетями при помощи групповых политик. Шифрование трафика беспроводной сети. Методы аутентификации пользователей в беспроводных сетях.

Практическая работа 11. Защита от закладок при разработке программ (семинар)

Задание. Подготовить доклад на три минуты по одной из следующих тем:

1. Почему при эксплуатации компьютерной системы важно знать ее параметры?
2. Какие стандартные средства Windows XP обеспечивают пользователю возможность определения параметров компьютерной системы?
3. Почему обеспечение бесперебойной работы дисковой системы компьютера является одной из основных мер обеспечения информационной безопасности?

Тест 2 по разделу «Администрирование сетевых служб».

Темы: Сканеры безопасности
Межсетевые экраны.
Виртуальные частные сети
Системы обнаружения вторжений
Защита беспроводных сетей

1. В соответствии с особенностями алгоритма вирусы можно разделить на два класса:
    1. вирусы изменяющие среду обитания, но не распространяющиеся
    2. **вирусы изменяющие среду обитания при распространении**
    3. **вирусы не изменяющие среду обитания при распространении**
    4. вирусы не изменяющие среду обитания и не способные к распространению в дальнейшем
2. К достоинствам технических средств защиты относятся:
    1. регулярный контроль
    2. **создание комплексных систем защиты**
    3. степень сложности устройства
    4. Все варианты верны
3. К тщательно контролируемым зонам относятся:
    1. **рабочее место администратора**
    2. **архив**
    3. **рабочее место пользователя**
4. К системам оповещения относятся:
    1. **инфракрасные датчики**

2. **электрические датчики**
3. электромеханические датчики
4. электрохимические датчики

5. К оборонительным системам защиты относятся:
   1. **проволочные ограждения**
   2. **звуковые установки**
   3. датчики
   4. **световые установки**
6. Охранное освещение бывает:
   1. **дежурное**
   2. световое
   3. **тревожное**
7. К национальным интересам РФ в информационной сфере относятся:
   1. **Реализация конституционных прав на доступ к информации**
   2. Защита информации, обеспечивающей личную безопасность
   3. Защита независимости, суверенитета, государственной и территориальной целостности
   4. Политическая экономическая и социальная стабильность
   5. Сохранение и оздоровлении окружающей среды
8. Информационная безопасность это:
   1. Состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз
   2. **Состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз**
   3. Состояние, когда не угрожает опасность информационным системам
   4. Политика национальной безопасности России
9. Наиболее распространенные угрозы информационной безопасности:
   1. **угрозы целостности**
   2. угрозы защищенности
   3. угрозы безопасности
   4. **угрозы доступности**
   5. **угрозы конфиденциальности**
10. Что относится к классу информационных ресурсов:
    1. **Документы**
    2. **Персонал**
    3. **Организационные единицы**
    4. **Промышленные образцы, рецептуры и технологии**
    5. **Научный инструментарий**
11. Гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена:
    1. **конфиденциальность**
    2. доступность
    3. аутентичность
    4. целостность
12. Устройства осуществляющие воздействие на человека путем передачи информации через внечувственное восприятие:
    1. Средства массовой информации
    2. Психотропные препараты
    3. Психотронные генераторы
    4. **Средства специального программно-технического воздействия**
13. Злонамеренные действия в нематериальной сфере могут быть подразделены на два класса, какие?

1. **Информационный саботаж**
2. **Физический саботаж**
3. Информационные инфекции

14. Что не относится к информационной инфекции:
    1. Троянский конь
    2. **Фальсификация данных**
    3. Черви
    4. Вирусы
    5. Логическая бомба

15. Деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения и несанкционированного доступа к защищаемой информации и от получения защищаемой информации:
    1. защита информации от непреднамеренного воздействия
    2. защита информации от несанкционированного воздействия
    3. защита информации от несанкционированного доступа
    4. ***защита от утечки информации**

16. Идентификатор субъекта доступа, который является его секретом:
    1. ***пароль**
    2. ключ
    3. электронно-цифровая подпись
    4. сертификат ключа подписи

17. Исследование возможности расшифрования информации без знания ключей:
    1. криптология
    2. **криптоанализ**
    3. взлом
    4. несанкционированный доступ

18. Состояние защищенности национальных интересов страны в информационной сфере от внутренних и внешних угроз это:
    1. **Информационная безопасность**
    2. Безопасность
    3. Национальная безопасность
    4. Защита информации

19. Охрана персональных данных, государственной, служебной и других видов информации ограниченного доступа это:
    1. Защита информации
    2. Компьютерная безопасность
    3. Защищенность информации
    4. Защищенность потребителей информации
    5. **Безопасность данных**

20. Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это:
    1. Информационная война
    2. **Информационное оружие**
    3. Информационное превосходство

21. Реализация конституционных прав и свобод человека, обеспечение личной безопасности, повышение качества и уровня жизни это:
    1. Интересы государства
    2. Интересы государства в информационной сфере
    3. **Интересы личности**
    4. Интересы личности в информационной сфере
    5. Интересы общества в информационной сфере

22. Информация, не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения, в преимущественное положение по сравнению с другими объектами:

1. Служебная информация
2. Коммерческая тайна
3. Банковская тайна
4. **Конфиденциальная информация**

23. Действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы.

1. Комплексное обеспечение информационной безопасности
2. Безопасность АС
3. Угроза информационной безопасности
4. **Атака на автоматизированную систему**
5. Политика безопасности

24. Вся накопленная информация об окружающей нас дейст вительности, зафиксированная на материальных носителях или в любой другой форме, обеспечивающая ее передачу во времени и пространстве между различными потребителями для решения научных, производст венных, управленческих и других задач

1. **Информационные ресурсы**
2. Информационная система
3. Информационная сфера
4. Информационные услуги
5. Информационные продукты

25. К какому уровню доступа информации относится следующая информация: «Информация, содержащая сведения об обстоятельствах и фактах, предоставляющих угрозу жизни, здоровью граждан …»

1. **Информация без ограничения права доступа**
2. Информация с ограниченным доступом
3. Информация, распространение которой наносит вред интересам общества
4. Объект интеллектуальной собственности
5. Иная общедоступная информация

26. Состояние защищенности при котором не угрожает опасность это:

1. Информационная безопасность
2. ***Безопасность**
3. Защита информации
4. Национальная безопасность

27. Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных:

1. **Защита информации**
2. Компьютерная безопасность
3. Защищенность информации
4. Защищенность потребителей информации

28. Особый вид отношений между государствами, при котором для разрешения существующих межгосударственных противоречий используются методы, средства и технологии силового воздействия на информационную сферу этих государств:

1. **Информационная война**
2. Информационное оружие
3. Информационное превосходство

29. Создание условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя , суверенитета и территориальной целостности это:

1. Интересы государства
2. **Интересы государства в информационной сфере**
3. Интересы личности
4. Интересы личности в информационной сфере
5. Интересы общества в информационной сфере

30. Информационно упорядоченная совокупность документов и информационных технологий, реализующая информационные процессы
1. Информационные ресурсы
2. **Информационная система**
3. Информационная сфера
4. Информационные услуги
5. Информационные продукты

31. К какому уровню доступа информации относится следующая информация: «Авторское право, патентное право…»
1. Информация без ограничения права доступа
2. Информация с ограниченным доступом
3. Информация, распространение которой наносит вред интересам общества
4. **Объект интеллектуальной собственности**
5. Иная общедоступная информация

32. Состояние защищенности многонационального народа как носителя суверенитета и единственного источника власти:
1. Информационная безопасность
2. Безопасность
3. Защита информации
4. **Национальная безопасность**

33. Защита от случайных и преднамеренных воздействий, чреватых нанесением ущерба владельцам или пользователям информации это:
1. Защита информации
2. Компьютерная безопасность
3. Защищенность информации
4. **Защищенность потребителей информации**

34. Средства уничтожения, искажения, или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним это:
1. Информационная война
2. **Информационное оружие**
3. Информационное превосходство

Тема 3.1 Развертывание инфраструктуры открытых ключей

Устный опрос: Предварительный этап — Подготовка принятия решения о развертывании PKI. Оценка готовности к развертыванию. Определение цели развертывания PKI. Определение сферы применения PKI. Выбор приоритетных сервисов безопасности. Анализ данных и приложений. Проектирование PKI — Формирование политики PKI. Модель доверия и архитектура PKI. Политика применения сертификатов. Выбор программного продукта или поставщика услуг PKI. Интеграция PKI с действующими системами и приложениями. Серверы и криптографическое аппаратное обеспечение. Смарт-карты и считыватели. Физическая среда. Управление и администрирование системы PKI.

Практическая работа 12. Защита от закладок при разработке программ (семинар)

Задание. Подготовить доклад на три минуты по одной из следующих тем:
1. Опишите причины нарушений в работе магнитных дисков.
2. Почему необходима процедура очистки диска?

3. Что такое фрагментация файла? Почему она возникает и как влияет на скорость операций чтения информации с диска?
4. Что такое фрагментация файла? В каких случаях рекомендуется выполнить дефрагментацию диска?

Тест 3 по разделу «Защита от закладок при разработке программ».
Темы: Развертывание инфраструктуры открытых ключей

1. Документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ:
    1. **Государственная тайна**
    2. Коммерческая тайна
    3. Банковская тайна
    4. Конфиденциальная информация

2. Свойство данных быть доступными для санкционированного пользования в произвольный момент времени, когда в обращении к ним возникает необходимость:
    1. Конфиденциальность
    2. Целостность
    3. **Доступность**
    4. Аутентичность
    5. Аппелируемость

3. Гарантия того, что в любой момент времени может быть произведена полноценная проверка любого компонента программного комплекса АС:
    1. Надежность
    2. Точность
    3. **Контролируемость**
    4. Устойчивость
    5. Доступность

4. Непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС:
    1. Принцип системности
    2. Принцип комплексности
    3. **Принцип непрерывной защиты**
    4. Принцип разумной достаточности
    5. Принцип гибкости системы

5. Возможные воздействия на АС, которые прямо или косвенно могут нанести ущерб ее безопасности:
    1. Комплексное обеспечение информационной безопасности
    2. Безопасность АС
    3. **Угрозы информационной безопасности**
    4. Атака на автоматизированную систему
    5. Политика безопасности

6. Совокупность информации, информационной структуры субъектов, осуществляющих сбор, формирование, распространение и использование информации, а так же системы регулирования возникающих при этом общественных отношений
    1. Информационные ресурсы
    2. Информационная система
    3. **Информационная сфера**
    4. Информационные услуги
    5. Информационные продукты

7. К какому уровню доступа информации относится следующая информация: «Ложная реклама, реклама со скрытыми вставками…»

1. Информация без ограничения права доступа
2. Информация с ограниченным доступом
3. **Информация, распространение которой наносит вред интересам общества**
4. Объект интеллектуальной собственности
5. Иная общедоступная информация

8. Защищенность страны от нападения извне, шпионажа, покушения на государственный и общественный строй:
1. Информационная безопасность
2. Безопасность
3. **Национальная безопасность**
4. Защита информации

9. Защищенность от негативных информационно-психологических и информационно-технических воздействий:
1. Защита информации
2. Компьютерная безопасность
3. Защищенность информации
4. **Защищенность потребителей информации**

10. Возможность сбора, обработки и распространения непрерывного потока информации при воспрещении использования информации противником это:
1. Информационная война
2. Информационное оружие
3. **Информационное превосходство**

11. Обобщение интересов личности в этой сфере, упрочнение демократии, создание правового государства это:
1. Интересы государства
2. Интересы государства в информационной сфере
3. Интересы личности в информационной сфере
4. **Интересы общества**
5. Интересы общества в информационной сфере

12. Защищаемые государством сведения в области военной, внешнеполитической и внешнеэкономической деятельности, распространение которых может нанести ущерб безопасности РФ.
1. **Государственная тайна**
2. Коммерческая тайна
3. Банковская тайна
4. Конфиденциальная информация

13. Гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор:
1. Конфиденциальность
2. Целостность
3. Доступность
4. **Аутентичность**
5. Аппелируемость

14. Гарантия того, что при умышленном внесении ошибок в пределах заранее оговоренных норм АС будет вести себя так, как оговорено заранее:
1. Надежность
2. Точность
3. Контролируемость
4. **Устойчивость**
5. Доступность

15. Согласование разнородных средств при построении целостной системы защиты, перекрывающий все существенные каналы реализации угроз и не содержащий слабых мест на стыках отдельных компонентов:

1. Принцип системности
2. **Принцип комплексности**
3. Принцип непрерывной защиты
4. Принцип разумной достаточности
5. Принцип гибкости системы

16. Защищенность АС от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, а также от попыток хищения, изменения или разрушения ее компонентов:

1. Комплексное обеспечение информационной безопасности
2. **Безопасность АС**
3. Угроза информационной безопасности
4. Атака на автоматизированную систему
5. Политика безопасности

17. Действие субъектов по обеспечению пользователей информационными продуктами:

1. Информационные ресурсы
2. Информационная система
3. Информационная сфера
4. **Информационные услуги**
5. Информационные продукты

18. К какому уровню доступа информации относится следующая информация: «Библиографические и опознавательные данные, личные характеристики , сведения о семейном положении, сведения об имущественном или финансовом состоянии…»

1. Информация без ограничения права доступа
2. **Информация с ограниченным доступом**
3. Информация, распространение которой наносит вред интересам общества
4. Объект интеллектуальной собственности
5. Иная общедоступная информация

19. Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов и требований:

1. Защищенность информации
2. **Защищаемая информация**
3. Защищенность потребителей информации
4. Защита информации

20. Действия предпринимаемые для достижения информационного превосходства в поддержке национальной информационной стратегии посредством воздействия на информацию и информационные системы противника:

1. **Информационная война**
2. Информационное оружие
3. Информационное превосходство

21. Гарантия неразглашения банковского счета, операций по счету и сведений о клиенте:

1. Государственная тайна
2. Коммерческая тайна
3. **Банковская тайна**
4. Конфиденциальная информация

22. Гарантия того, что при необходимости можно будет доказать, что автором сообщения является именно тот человек, который заявлен как ее автор и ни кто другой:

1. Конфиденциальность
2. Целостность
3. Доступность

4. Аутентичность
5. **Аппелируемость**

23. Системный подход к защите компьютерных систем предполагающий необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов:
1. **Принцип системности**
2. Принцип комплексности
3. Принцип непрерывной защиты
4. Принцип разумной достаточности
5. Принцип гибкости системы

24. Область науки и техники, охватывающая совокупность криптографических, программно-аппаратных, технических, правовых, организационных методов и средств обеспечения безопасности информации при ее обработке, хранении и передаче с использованием современных информационных технологий:
1. **Комплексное обеспечение информационной безопасности**
2. Безопасность АС
3. Угроза безопасности
4. Атака на автоматизированную систему
5. Политика безопасности

25. Документированная информация, подготовленная в соответствии с потребностями пользователей и предназначенная или применяемая для удовлетворения потребностей пользователей:
1. Информационные ресурсы
2. Информационная система
3. Информационная сфера
4. Информационные услуги
5. **Информационные продукты**

26. К какому уровню доступа информации относится следующая информация: «Информация в области работ по хранению, перевозке, уничтожению химического оружия – сведения о состоянии здоровья граждан и объектов окружающей среды в районах размещения объектов по уничтожению химического оружия…»
1. Информация без ограничения права доступа
2. **Информация с ограниченным доступом**
3. Информация, распространение которой наносит вред интересам общества
4. Объект интеллектуальной собственности
5. Иная общедоступная информация

27. Соотнесите интересы в области информационной безопасности:
1. Национальные интересы
2. Интересы личности
3. Интересы государства
4. Интересы общества

1. состоят в реализации конституционных прав и свобод [2], в обеспечении личной безопасности, в повышении качества и уровня жизни, в физическом, духовном и интеллектуальном развитии человека и гражданина
2. обеспечиваются институтами государствен ной власти, осуществляющими свои функции, в том числе во взаимодей ствии с действующими на основе Конституции РФ и законодательства РФ общественными организациями
3. состоят в незыблемости конституционного строя, суверенитета и территориальной целостности России, в политиче ской, экономической и социальной стабильности, в

безусловном обеспе чении законности и поддержании правопорядка, в развитии равноправно го и взаимовыгодного международного сотрудничества.

4. состоят в упрочении демократии, в создании правового, социального государства, в достижении и поддержании обще ственного согласия, в духовном обновлении России.

ОТВЕТ: 1-2; 2-1; 3-3; 4-4.

28. Соотнесите основные методы получения паролей:
    1. метод тотального перебора
    2. словарная атака
    3. получение паролей из самой системы на основе программной и аппаратной реализации конкретной системы
    4. проверка паролей, устанавливаемых в системах по умолчанию
    1. для перебора используется словарь наиболее вероятных ключей
    2. двумя возможностями выяснения пароля являются: несанкционированный доступ к носителю, содержащему пароли, либо использование уязвимостей
    3. опробываются все ключи последовательно, один за другим
    4. пароль, установленный фирмой-разработчиком по умолчанию, остается основным паролем в системе

ОТВЕТ: 1-3; 2-1; 3-2; 4-4;

29. Соотнесите принципы информационной безопасности, определенные Гостехкомиссией
    1. Принцип системности
    2. Принцип комплексности
    3. Принцип непрерывности защиты
    4. Гибкость системы защиты
    5. Разумная достаточность
    1. правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможно го ущерба были бы приемлемыми
    2. непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла автоматизированных систем
    3. предполагает согласование разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов
    4. освобождает владельца автоматизированных систем от необходимости принятия кардинальных мер по полной замене средств защиты на новые.
    5. предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов

ОТВЕТ: 1-5; 2-3; 3-2; 4-4; 5-1;

30. Соотнесите основные понятия в области информационной безопасности:
    1. Атака
    2. Уязвимость автоматизированных систем
    3. Угроза безопасности автоматизированных систем
    4. Защищенная система
    1. некоторое неудачное свойство системы, которое делает возможным возникновение и реализацию угрозы
    2. система со средствами защиты, которые успешно и эффективно противостоят угрозам безопасности

3. возможные воздействия на автоматизированных систем, которые прямо или косвенно могут нанести ущерб ее безопасности
4. действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы

ОТВЕТ: 1-4; 2-1; 3-3; 4-2;

31. Соотнесите функции, выполняемые техническими средствами защиты:
    1. внешняя защита
    2. опознавание
    3. внутренняя защита
    1. защита от воздействия дестабилизирующих факторов, проявляющихся непосредственно в средствах обработки информации
    2. защита от воздействия дестабилизирующих факторов, проявляющихся за пределами основных средств автоматизированные системы обработки данных
    3. специфическая группа средств, предназначен ных для опознавания людей по различным индивидуальным харак теристикам

ОТВЕТ: 1-2; 2-3; 3-1

32. Соотнесите степени сложности устройств:
    1. простые устройства
    2. системы
    3. сложные устройства
        1. комбинированные агрегаты, состоя щие из некоторого количества простых устройств, способные к осу ществлению сложных процедур защиты;
        2. несложные приборы и приспособле ния, выполняющие отдельные процедуры защиты;
        3. законченные технические комплексы, способные осуществлять некоторую комбинированную процедуру защиты, имеющую самостоятельное значение;

ОТВЕТ: 1-2; 2-3; 3-1;

33. Соотнесите основные виды угроз для автоматизированных систем:
    1. Угроза нарушения конфиденциальности
    2. Угроза отказа служб
    3. Угроза нарушения целостности
        1. Любое умышленное изменение информации, хранящейся в ВС или передаваемой от одной системы в другую
        2. Возникает всякий раз, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу автоматизированных систем
        3. Заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней

ОТВЕТ: 1-3; 2-2; 3-1

34. Соотнесите классификацию угроз по ряду признаков:
    1. по природе возникновения
    2. по непосредственному источнику
    3. по степени воздействия на автоматизированные системы
    4. по способу доступа к ресурсам автоматизированных систем
    1. пассивные и активные

2. направленные на использование прямого стандартного пути доступа к ресурсам и направленные на использование скрытого нестандартного доступа к ресурсам автоматизированных систем
3. естественные или искусственные
4. природная среда, человек, санкционированные программные средства и несанкционированные программные средства

ОТВЕТ: 1-3; 2-4; 3-3;4-1

Тема 4.1 Организация резервного копирования на серверах Windows

Устный опрос: Оборудование для архивации. Создание плана резервного копирования. Выбор архивируемых данных. Типы архивации.

Практическая работа 13. Защита от закладок при разработке программ (семинар)

Задание. Подготовить доклад на три минуты по одной из следующих тем:

1. С какой целью выполняется архивация данных компьютера?
2. Что такое дискета аварийного восстановления? Какой программой она создается?
3. Какие вы знаете программы восстановления информации на магнитных дисках?

Практическая работа 14. Профилактика заражения вирусами компьютерных систем (семинар)

Задание. Подготовить доклад на три минуты по одной из следующих тем:

1. Что такое компьютерный вирус? Какими свойствами обладают компьютерные вирусы?
2. По каким признакам классифицируют компьютерные вирусы? Перечислите типы вирусов.
3. Какие вирусы называются резидентными и в чем особенность таких вирусов?
4. Каковы отличия вирусов-репликаторов, стелс - вирусов, мутантов и «троянских» программ?
5. Опишите схему функционирования загрузочного вируса.
6. Опишите схему функционирования файлового вируса.
7. Опишите схему функционирования загрузочно-файловых вирусов, особенности.

Тема 4.2 RAID и зеркалирование

Устный опрос: Классификация RAID-массивов. Комбинированные уровни RAID. Программный RAID в Windows. Программный RAID в Linux.

Практическая работа 15. Профилактика заражения вирусами компьютерных систем (семинар)

Задание. Подготовить доклад на три минуты по одной из следующих тем:

1. Что такое полиморфный вирус? Почему этот тип вирусов считается наиболее опасным?
2. Каковы причины появления компьютерных вирусов. Приведите примеры широко известных вирусов.
3. Существует ли в мире и в РФ уголовная ответственность за создание и распространение компьютерных вирусов?
4. Каковы пути проникновения вирусов в компьютер и признаки заражения компьютера вирусом?
5. Каковы способы обнаружения вирусов и антивирусной профилактики?
6. Перечислите основные меры по защите от компьютерных вирусов.
7. Опишите назначение антивирусных программ различных типов.
8. Назовите примеры современных антивирусных программ и опишите их

Практическая работа 16. Виды угроз информационной безопасности Российской Федерации (семинар)

Задание. Подготовить доклад на три минуты по одной из следующих тем:

1. Перечислите виды угроз безопасности информационного общества.
2. В чем заключается угроза раскрытия информации? Какие еще угрозы Вы знаете?
3. Что положено в основу дискреционной модели доступа?
4. Раскройте понятие троянской программы в контексте защиты информации в вычислительной системе.

Вопросы к экзамену

Теоретические задания

1. Проблема обеспечения безопасности в информационных системах.
2. Специфика эксплуатации защищенных информационных систем
3. Концепция проектирования системы защиты информационных систем.
4. Общий состав работ на этапе эксплуатации IT-систем
5. Требования по защите информационных систем, устанавливаемые законодательством РФ
6. Сканеры безопасности
7. Межсетевые экраны
8. Виртуальные частные сети.
9. Системы обнаружения вторжений.
10. Защита беспроводных сетей
11. Развертывание инфраструктуры открытых ключей.
12. Организация резервного копирования на серверах Windows
13. RAID и зеркалирование
14. Межсетевые экраны.
15. Требования по защите информационных систем, устанавливаемые законодательством РФ
16. Проблема обеспечения безопасности в информационных системах.
17. Специфика эксплуатации защищенных информационных систем.
18. Задачи распределения ключей.
19. Защита беспроводных сетей
20. RAID и зеркалирование
21. Концепция проектирования системы защиты информационных систем
22. Системы обнаружения вторжений.
23. Защита беспроводных сетей
24. Организация резервного копирования на серверах Windows.
25. Общий состав работ на этапе эксплуатации IT-систем.

Практические задания

26. Зашифровать заданный преподавателем текст шифрованием методом замены (Шифр Цезаря). Расшифровать заданный преподавателем текст зашифрованный шифром Цезаря.
27. Зашифровать заданный преподавателем текст с помощью подстановочного шифра (Шифр Виженера).
28. Зашифровать заданный преподавателем текст с помощью подстановочного шифра (Шифр Виженера).
29. Зашифровать заданный преподавателем текст с помощью шифра простой перестановки.

30. Зашифровать заданный преподавателем текст с помощью шифра одноалфавитной замены.
31. Зашифровать заданный преподавателем текст с помощью шифра Гронсфельда.
32. Зашифровать заданный преподавателем текст с помощью шифра двойного квадрата
33. Зашифровать заданный преподавателем текст с помощью шифра ГОСТ 28147-89.
34. Зашифровать заданный преподавателем текст с помощью шифра Эль Гамаля.
35. Задачи и алгоритмы электронной подписи
36. Задачи распределения ключей.
37. Зашифровать заданный преподавателем текст с помощью шифра RSA.
38. Зашифровать заданный преподавателем текст с помощью шифрования DES.
39. Зашифровать заданный преподавателем текст с помощью шифра многоалфавитной замены.
40. Зашифровать заданный преподавателем текст с помощью шифра одиночной перестановки по ключу.
41. Зашифровать заданный преподавателем текст с шифрованием с помощью магического квадрата.
42. Зашифровать заданный преподавателем текст с помощью шифра RSA.
43. Зашифровать заданный преподавателем текст с помощью шифра ГОСТ 28147-89.
44. Зашифровать заданный преподавателем текст с помощью шифра Гронсфельда.
45. Зашифровать заданный преподавателем текст с помощью подстановочного шифра (Шифр Виженера).
46. Зашифровать заданный преподавателем текст с помощью шифра простой перестановки.
47. Зашифровать заданный преподавателем текст с помощью подстановочного шифра (Шифр Виженера).
48. Зашифровать заданный преподавателем текст с помощью шифрования DES.
49. Зашифровать заданный преподавателем текст с помощью шифра двойного квадрата
50. Зашифровать заданный преподавателем текст с помощью подстановочного шифра (Шифр Виженера).

7. Регламент междисциплинарного курса.

Экзамен нацелен на комплексную проверку освоения междисциплинарного курса. Экзамен проводится в двух формах: в устной форме по всем темам курса и выполнение практического задания. Обучающемуся даётся время на подготовку. Оценивается владение материалом, его системное освоение, способность применять нужные знания, навыки и умения при анализе проблемных ситуаций.

Компетенции	Планируемые результаты обучения	Критерии оценивания результатов обучения (баллы)			
		2	3	4	5
ОК-1	Знать основные понятия информационных систем, жизненный цикл, проблемы обеспечения технологической безопасности	Не знает Допускает грубые ошибки	Демонстрирует частичные знания без грубых ошибок	Знает достаточно в базовом объёме	Демонстрирует высокий уровень знаний

	информационных систем, требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования, оперативные методы повышения безопасности функционирования программных средств и баз данных;				
	Уметь устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту	Не умеет Демонстрирует частичные умения, допуская грубые ошибки	Демонстрирует частичные умения без грубых ошибок	Умеет применять знания на практике в базовом объёме	Демонстрирует высокий уровень умений
	Иметь практический опыт обслуживания сетевой инфраструктуры, восстановления работоспособности сети после сбоя;	Не владеет Демонстрирует низкий уровень владения, допуская грубые ошибки	Демонстрирует частичные владения без грубых ошибок	Владеет базовыми приёмами	Демонстрирует владения на высоком уровне
ОК-2	Знать основные требования к средствам и видам тестирования для определения технологической безопасности	Не знает Допускает грубые ошибки	Демонстрирует частичные знания без грубых ошибок	Знает достаточно в базовом объёме	Демонстрирует высокий уровень знаний

	информационных систем				
	Уметь организовывать защиту информации в автоматизированных системах обработки данных;	Не умеет Демонстрирует частичные умения, допуская грубые ошибки	Демонстрирует частичные умения без грубых ошибок	Умеет применять знания на практике в базовом объёме	Демонстрирует высокий уровень умений
	Иметь практический опыт удаленного администрирования и восстановления работоспособности сетевой инфраструктуры;	Не владеет Демонстрирует низкий уровень владения, допуская грубые ошибки	Демонстрирует частичные владения без грубых ошибок	Владеет базовыми приёмами	Демонстрирует владения на высоком уровне
ОК- 3	Знать средства защиты информации в автоматизированных системах обработки данных;	Не знает Допускает грубые ошибки	Демонстрирует частичные знания без грубых ошибок	Знает достаточно в базовом объёме	Демонстрирует высокий уровень знаний
	Уметь использовать антивирусные программы.	Не умеет Демонстрирует частичные умения, допуская грубые ошибки	Демонстрирует частичные умения без грубых ошибок	Умеет применять знания на практике в базовом объёме	Демонстрирует высокий уровень умений
	Иметь практический опыт организации бесперебойной работы системы по резервному копированию и восстановлению информации;	Не владеет Демонстрирует низкий уровень владения, допуская грубые ошибки	Демонстрирует частичные владения без грубых ошибок	Владеет базовыми приёмами	Демонстрирует владения на высоком уровне

ОК- 4	Знать компьютерные вирусы и антивирусные программы;	Не знает Допускает грубые ошибки	Демонстрирует частичные знания без грубых ошибок	Знает достаточно в базовом объёме	Демонстрирует высокий уровень знаний
	Уметь устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту	Не умеет Демонстрирует частичные умения, допуская грубые ошибки	Демонстрирует частичные умения без грубых ошибок	Умеет применять знания на практике в базовом объёме	Демонстрирует высокий уровень умений
	Иметь практический опыт поддержки пользователей сети, настройки аппаратного и программного обеспечения сетевой инфраструктуры	Не владеет Демонстрирует низкий уровень владения, допуская грубые ошибки	Демонстрирует частичные владения без грубых ошибок	Владеет базовыми приёмами	Демонстрирует владения на высоком уровне
ОК - 5	Знать политику информационной безопасности;	Не знает Допускает грубые ошибки	Демонстрирует частичные знания без грубых ошибок	Знает достаточно в базовом объёме	Демонстрирует высокий уровень знаний
	Уметь организовывать защиту информации в автоматизированных системах обработки	Не умеет Демонстрирует частичные умения, допуская	Демонстрирует частичные умения без грубых ошибок	Умеет применять знания на практике в базовом объёме	Демонстрирует высокий уровень умений

	данных;	грубые ошибки			
	Иметь практический опыт обслуживания сетевой инфраструктуры, восстановления работоспособности сети после сбоя;	Не владеет Демонстрирует низкий уровень владения, допуская грубые ошибки	Демонстрирует частичные владения без грубых ошибок	Владеет базовыми приёмами	Демонстрирует владения на высоком уровне
ОК- 6	Знать стандарты информационной безопасности.	Не знает Допускает грубые ошибки	Демонстрирует частичные знания без грубых ошибок	Знает достаточно в базовом объёме	Демонстрирует высокий уровень знаний
	Уметь использовать антивирусные программы.	Не умеет Демонстрирует частичные умения, допуская грубые ошибки	Демонстрирует частичные умения без грубых ошибок	Умеет применять знания на практике в базовом объёме	Демонстрирует высокий уровень умений
	Иметь практический опыт удаленного администрирования и восстановления работоспособности сетевой инфраструктуры;	Не владеет Демонстрирует низкий уровень владения, допуская грубые ошибки	Демонстрирует частичные владения без грубых ошибок	Владеет базовыми приёмами	Демонстрирует владения на высоком уровне
ОК- 7	Знать основные понятия информационных систем, жизненный цикл, проблемы обеспечения	Не знает Допускает грубые ошибки	Демонстрирует частичные знания без грубых ошибок	Знает достаточно в базовом объёме	Демонстрирует высокий уровень знаний

	технологической безопасности информационных систем, требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования, оперативные методы повышения безопасности функционирования программных средств и баз данных;				
	Уметь устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту	Не умеет Демонстрирует частичные умения, допуская грубые ошибки	Демонстрирует частичные умения без грубых ошибок	Умеет применять знания на практике в базовом объёме	Демонстрирует высокий уровень умений
	Иметь практический опыт организации бесперебойной работы системы по резервному копированию и восстановлению информации;	Не владеет Демонстрирует низкий уровень владения, допуская грубые ошибки	Демонстрирует частичные владения без грубых ошибок	Владеет базовыми приёмами	Демонстрирует владения на высоком уровне

ОК-8	Знать основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем	Не знает Допускает грубые ошибки	Демонстрирует частичные знания без грубых ошибок	Знает достаточно в базовом объёме	Демонстрирует высокий уровень знаний
	Уметь организовывать защиту информации в автоматизированных системах обработки данных;	Не умеет Демонстрирует частичные умения, допуская грубые ошибки	Демонстрирует частичные умения без грубых ошибок	Умеет применять знания на практике в базовом объёме	Демонстрирует высокий уровень умений
	Иметь практический опыт поддержки пользователей сети, настройки аппаратного и программного обеспечения сетевой инфраструктуры	Не владеет Демонстрирует низкий уровень владения, допуская грубые ошибки	Демонстрирует частичные владения без грубых ошибок	Владеет базовыми приёмами	Демонстрирует владения на высоком уровне
ОК-9	Знать средства защиты информации в автоматизированных системах обработки данных;	Не знает Допускает грубые ошибки	Демонстрирует частичные знания без грубых ошибок	Знает достаточно в базовом объёме	Демонстрирует высокий уровень знаний
	Уметь использовать	Не умеет	Демонстрирует частичные	Умеет применять	Демонстрирует высокий

	антивирусные программы.	Демонстрирует частичные умения, допуская грубые ошибки	умения без грубых ошибок	знания на практике в базовом объёме	уровень умений
	Иметь практический опыт обслуживания сетевой инфраструктуры, восстановления работоспособности сети после сбоя;	Не владеет Демонстрирует низкий уровень владения, допуская грубые ошибки	Демонстрирует частичные владения без грубых ошибок	Владеет базовыми приёмами	Демонстрирует владения на высоком уровне
ПК- 3.1	Знать средства защиты информации в автоматизированных системах обработки данных	Не знает Допускает грубые ошибки	Демонстрирует частичные знания без грубых ошибок	Знает достаточно в базовом объёме	Демонстрирует высокий уровень знаний
	Уметь устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту	Не умеет Демонстрирует частичные умения, допуская грубые ошибки	Демонстрирует частичные умения без грубых ошибок	Умеет применять знания на практике в базовом объёме	Демонстрирует высокий уровень умений
	Иметь практический опыт поддержки пользователей сети, настройки аппаратного и	Не владеет Демонстрирует низкий уровень владения, допуская грубые ошибки	Демонстрирует частичные владения без грубых ошибок	Владеет базовыми приёмами	Демонстрирует владения на высоком уровне

	программного обеспечения сетевой инфраструктуры.				
ПК- 3.2	Знать основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем	Не знает Допускает грубые ошибки	Демонстрирует частичные знания без грубых ошибок	Знает достаточно в базовом объёме	Демонстрирует высокий уровень знаний
	Уметь устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту	Не умеет Демонстрирует частичные умения, допуская грубые ошибки	Демонстрирует частичные умения без грубых ошибок	Умеет применять знания на практике в базовом объёме	Демонстрирует высокий уровень умений
	Иметь практический опыт организации бесперебойной работы системы по резервному копированию и восстановлению информации	Не владеет Демонстрирует низкий уровень владения, допуская грубые ошибки	Демонстрирует частичные владения без грубых ошибок	Владеет базовыми приёмами	Демонстрирует владения на высоком уровне
ПК- 3.3	Знать стандарты информационной безопасности	Не знает Допускает грубые ошибки	Демонстрирует частичные знания без грубых ошибок	Знает достаточно в базовом объёме	Демонстрирует высокий уровень знаний

	Уметь устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту	Не умеет Демонстрирует частичные умения, допуская грубые ошибки	Демонстрирует частичные умения без грубых ошибок	Умеет применять знания на практике в базовом объёме	Демонстрирует высокий уровень умений
	Иметь практический опыт организации бесперебойной работы системы по резервному копированию и восстановлению информации;	Не владеет Демонстрирует низкий уровень владения, допуская грубые ошибки	Демонстрирует частичные владения без грубых ошибок	Владеет базовыми приёмами	Демонстрирует владения на высоком уровне
ПК- 3.4	Знать стандарты информационной безопасности	Не знает Допускает грубые ошибки	Демонстрирует частичные знания без грубых ошибок	Знает достаточно в базовом объёме	Демонстрирует высокий уровень знаний
	Уметь организовывать защиту информации в автоматизированных системах обработки данных;	Не умеет Демонстрирует частичные умения, допуская грубые ошибки	Демонстрирует частичные умения без грубых ошибок	Умеет применять знания на практике в базовом объёме	Демонстрирует высокий уровень умений
	Иметь практический опыт организации бесперебойной работы системы по резервному копированию и восстановлению информации;	Не владеет Демонстрирует низкий уровень владения, допуская грубые ошибки	Демонстрирует частичные владения без грубых ошибок	Владеет базовыми приёмами	Демонстрирует владения на высоком уровне

ПК-3.5	Знать стандарты информационной безопасности	Не знает Допускает грубые ошибки	Демонстрирует частичные знания без грубых ошибок	Знает достаточно в базовом объёме	Демонстрирует высокий уровень знаний
	Уметь использовать антивирусные программы	Не умеет Демонстрирует частичные умения, допуская грубые ошибки	Демонстрирует частичные умения без грубых ошибок	Умеет применять знания на практике в базовом объёме	Демонстрирует высокий уровень умений
	Иметь практический опыт поддержки пользователей сети, настройки аппаратного и программного обеспечения сетевой инфраструктуры	Не владеет Демонстрирует низкий уровень владения, допуская грубые ошибки	Демонстрирует частичные владения без грубых ошибок	Владеет базовыми приёмами	Демонстрирует владения на высоком уровне
ПК-3.6	Знать основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем	Не знает Допускает грубые ошибки	Демонстрирует частичные знания без грубых ошибок	Знает достаточно в базовом объёме	Демонстрирует высокий уровень знаний
	Уметь организовывать защиту информации в автоматизированных системах обработки данных;	Не умеет Демонстрирует частичные умения, допуская грубые ошибки	Демонстрирует частичные умения без грубых ошибок	Умеет применять знания на практике в базовом объёме	Демонстрирует высокий уровень умений
	Иметь	Не владеет	Демонстрирует	Владеет	Демонстрирует

	практический опыт поддержки пользователей сети, настройки аппаратного и программного обеспечения сетевой инфраструктуры	Демонстрирует низкий уровень владения, допуская грубые ошибки	частичные владения без грубых ошибок	базовыми приёмами	владения на высоком уровне

8. Таблица соответствия компетенций, критериев оценки их освоения, оценочных средств и этапов их формирования

Индекс компетенции	**Расшифровка компетенции**	**Показатель формирования компетенции для данной междисциплинарного курса**	**Оценочные средства**	**Этапы формирования компетенции**
1	2	3	4	5
ОК 1	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.	Знать основные понятия информационных систем, жизненный цикл, проблемы обеспечения технологической безопасности информационных систем, требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования, оперативные методы повышения безопасности функционирования программных средств и баз данных; Уметь устанавливать, тестировать и эксплуатировать	Устный опрос по темам: 1.1-1.6, 2.1-2.5, 3.1, 4.1-4.2	1 этап
			Теоретические вопросы к экзамену 1-25	2 этап

		информационные системы, согласно технической документации, обеспечивать антивирусную защиту Иметь практический опыт обслуживания сетевой инфраструктуры, восстановления работоспособности сети после сбоя		
ОК 2	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	Знать основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем Уметь организовывать защиту информации в автоматизированных системах обработки данных; Иметь практический опыт удаленного администрирования и восстановления работоспособности сетевой инфраструктуры;	Устный опрос по темам: 1.1-1.6, 2.1-2.5, 3.1, 4.1-4.2	1 этап
			Теоретические вопросы к экзамену 1-25	2 этап
ОК 3	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность	Знать средства защиты информации в автоматизированных системах обработки данных; Уметь использовать	Устный опрос по темам: 1.1-1.6, 2.1-2.5, 3.1, 4.1-4.2	1 этап

		антивирусные программы. Иметь практический опыт организации бесперебойной работы системы по резервному копированию и восстановлению информации;		
			Теоретические вопросы к экзамену 1-25	2 этап
ОК 4	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития	Знать компьютерные вирусы и антивирусные программы; Уметь устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту Иметь практический опыт поддержки пользователей сети, настройки аппаратного и программного обеспечения сетевой инфраструктуры	Устный опрос по темам: 1.1-1.6, 2.1-2.5, 3.1, 4.1-4.2	1 этап
			Теоретические вопросы к экзамену 1-25	2 этап
ОК 5	Использовать информационно-коммуникационные технологии в профессиональной деятельности	Знать политику информационной безопасности; Уметь организовывать	Устный опрос по темам: 1.1-1.6, 2.1-2.5, 3.1, 4.1-4.2	1 этап

		защиту информации в автоматизированных системах обработки данных; Иметь практический опыт обслуживания сетевой инфраструктуры, восстановления работоспособности сети после сбоя;	Теоретические вопросы к экзамену 1-25	2 этап
ОК 6	Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями	Знать стандарты информационной безопасности. Уметь использовать антивирусные программы. Иметь практический опыт удаленного администрирования и восстановления работоспособности сетевой инфраструктуры;	Устный опрос по темам: 1.1-1.6, 2.1-2.5, 3.1, 4.1-4.2	1 этап
			Теоретические вопросы к экзамену 1-25	2 этап

ОК 7	Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий..	Знать основные понятия информационных систем, жизненный цикл, проблемы обеспечения технологической безопасности информационных систем, требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования, оперативные методы повышения безопасности функционирования программных средств и баз данных; Уметь устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту Иметь практический опыт организации бесперебойной работы системы по резервному копированию и восстановлению информации;	Устный опрос по темам: 1.1-1.6, 2.1-2.5, 3.1, 4.1-4.2	1 этап
			Теоретические вопросы к экзамену 1-25	2 этап

ОК-8	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации	Знать основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем Уметь организовывать защиту информации в автоматизированных системах обработки данных; Иметь практический опыт поддержки пользователей сети, настройки аппаратного и программного обеспечения сетевой инфраструктуры	Устный опрос по темам: 1.1-1.6, 2.1-2.5, 3.1, 4.1-4.2	1 этап
			Теоретические вопросы к экзамену 1-25	2 этап
ОК-9	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	Знать средства защиты информации в автоматизированных системах обработки данных; Уметь использовать антивирусные программы. Иметь практический опыт обслуживания сетевой инфраструктуры, восстановления работоспособности сети после сбоя;	Устный опрос по темам: 1.1-1.6, 2.1-2.5, 3.1, 4.1-4.2	1 этап
			Теоретические вопросы к экзамену 1-25	2 этап

ПК 3.1	Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей.	Знать средства защиты информации в автоматизированных системах обработки данных Уметь устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту Иметь практический опыт поддержки пользователей сети, настройки аппаратного и программного обеспечения сетевой инфраструктуры.	Практические работы 1-16	1 этап
			Тесты 1-3	2 этап
			Практические вопросы к экзамену 26-50	3 этап
ПК 3.2	Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях	Знать основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем Уметь устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту Иметь практический опыт организации	Практические работы 1-16	1 этап
			Тесты 1-3	2 этап
			Практические вопросы к экзамену 26-50	3 этап

		бесперебойной работы системы по резервному копированию и восстановлению информации		
ПК 3.3	Эксплуатация сетевых конфигураций.	Знать стандарты информационной безопасности Уметь устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту Иметь практический опыт организации бесперебойной работы системы по резервному копированию и восстановлению информации;	Практические работы 1-16	1 этап
			Тесты 1-3	2 этап
			Практические вопросы к экзамену 26-50	3 этап
ПК 3.4	Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации	Знать стандарты информационной безопасности Уметь организовывать защиту информации в автоматизированных системах обработки данных; Иметь практический опыт организации бесперебойной работы системы по резервному копированию и восстановлению информации;	Практические работы 1-16	1 этап
			Тесты 1-3	2 этап

			Практические вопросы к экзамену 26-50	3 этап
ПК 3.5	Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль поступившего из ремонта оборудования	Знать стандарты информационной безопасности Уметь использовать антивирусные программы Иметь практический опыт поддержки пользователей сети, настройки аппаратного и программного обеспечения сетевой инфраструктуры	Практические работы 1-16	1 этап
			Тесты 1-3	2 этап
			Практические вопросы к экзамену 26-50	3 этап
ПК 3.6	Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.	Знать основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем Уметь организовывать защиту информации в автоматизированных системах обработки данных; Иметь практический опыт поддержки пользователей сети, настройки аппаратного и программного обеспечения сетевой	Практические работы 1-16	1 этап
			Тесты 1-3	2 этап
			Практические вопросы к экзамену 26-50	3 этап

		инфраструктуры		

9. Методические указания для обучающихся при освоении междисциплинарного курса (модуля)

Работа на практических занятиях предполагает активное участие в осуждении выдвинутых в рамках тем вопросов. Для подготовки к занятиям рекомендуется обращать внимание на проблемные вопросы, затрагиваемые преподавателем в лекции, и группировать информацию вокруг них. Желательно выделять в используемой литературе постановки вопросов, на которые разными авторам могут быть даны различные ответы. На основании постановки таких вопросов следует собирать аргументы в пользу различных вариантов решения поставленных проблем.

В текстах авторов, таким образом, следует выделять следующие компоненты:

- постановка проблемы;
- варианты решения;
- аргументы в пользу тех или иных вариантов решения.

На основе выделения этих элементов проще составлять собственную аргументированную позицию по рассматриваемому вопросу.

При работе с терминами необходимо обращаться к словарям, в том числе доступным в Интернете, например на сайте http://dic.academic.ru.

При подготовке к практическим работам может понадобиться материал, изучавшийся ранее, поэтому стоит обращаться к соответствующим источникам (учебникам).

Практические работы решаются в группе с обсуждением хода решения, применяемых способов, проверкой результатов и проведением работы над ошибками.

Домашняя работа и задания могут быть индивидуальными и общими.

При подготовке к экзамену необходимо опираться на лекции, а также на источники, которые разбирались на практических занятиях в течение семестра.

10. Учебно-методическое и информационное обеспечение междисциплинарного курса

10.1. Основная литература

1. Корпоративные информационные системы управления: Учебник / Под науч. ред. Н.М. Абдикеева, О.В. Китовой. - М.: НИЦ ИНФРА-М, 2014. - 464 с.: 60x90 1/16 + (Доп. мат. znanium.com). - (ВО: Магистратура). (переплет) ISBN 978-5-16-003860-5, 500 экз.
2. Информационные системы предприятия: Учебное пособие / А.О. Варфоломеева, А.В. Коряковский, В.П. Романов. - М.: НИЦ ИНФРА-М, 2016. - 283 с.: 60x90 1/16. - (Высшее образование: Бакалавриат) (Переплёт 7БЦ) ISBN 978-5-16-005549-7
3. Проектирование информационных систем: Учебное пособие / В.В. Коваленко. - М.: Форум: НИЦ ИНФРА-М, 2014. - 320 с.: 60x90 1/16. - (Высшее образование). (переплет) ISBN 978-5-91134-549-5, 300 экз.
4. Аверченков, В. И. Аудит информационной безопасности [электронный ресурс] : учеб. пособие для вузов / В. И. Аверченков. – 2-е изд., стереотип. – М. : Флинта, 2051. – 269 с. - ISBN 978-5-9765-1256-6
5. Семенов, А. Б. Администрирование структурированных кабельных систем [Электронный ресурс] / А. Б. Семенов. - М.: ДМК Пресс; Компания АйТи, 2015. - 192 с.: ил. - ISBN 978-5-94074-431-3.

6. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с.: ил.; 60x90 1/16. - (Профессиональное образование). (переплет) ISBN 978-5-8199-0331-5, 1000 экз.
7. Жуков, В. Г. Беспроводные локальные сети стандартов IEEE 802.11 a/b/g [Электронный ресурс] : учеб. пособие / В. Г. Жуков. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 128 с.
8. Комплексная защита информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 592 с.: ил.; 70x100 1/16. - (Высшее образование). (переплет) ISBN 978-5-8199-0411-4
9. Райтман, М. А. Установка и настройка Windows 7 для максимальной производительности [Электронный ресурс] / М.А. Райтман . — СПб.: БХВ-Петербург, 2014. — 368.: ил. - ISBN 978-5-9775-0405-8

10.2. Дополнительная литература:

1. Мельников, В.П. Информационная безопасность и защита информации : учеб.пособие для студ. высш. учеб. заведений / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова. – 3-е изд., стер. – М.: Издательский центр «Академия», 2013. – 336 с.ISBN978-5-7695-4884-0

11. Материально-техническое и программное обеспечение междисциплинарного курса

Освоение междисциплинарного курса «Технология разработки и защиты баз данных» предполагает использование следующего материально-технического обеспечения: принтер и ксерокс для раздаточных материалов.

Учебно-методическая литература для данной междисциплинарного курса имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен обучающимся. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов среднего профессионального образования нового поколения.

Учебно-методическая литература для данной междисциплинарного курса имеется в наличии в электронно-библиотечной системе Издательства "Лань", доступ к которой предоставлен обучающимся. ЭБС Издательства "Лань" включает в себя электронные версии книг издательства "Лань" и других ведущих издательств учебной литературы, а также электронные версии периодических изданий по естественным, техническим и гуманитарным наукам. ЭБС Издательства "Лань" обеспечивает доступ к научной, учебной литературе и научным периодическим изданиям.

12. Методы обучения для обучающихся инвалидов и лиц с ограниченными возможностями здоровья.

В образовательном процессе используются социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в

установлении полноценных межличностных отношений с другими обучающимися, создании комфортного психологического климата в студенческой группе.

Условия обучения инвалидов и лиц с ограниченными возможностями здоровья:

- учебные аудитории, в которых проводятся занятия со студентами с нарушениями слуха, оборудованы мультимедийной системой (ПК и проектор), компьютерные тифлотехнологии базируются на комплексе аппаратных и программных средств, обеспечивающих преобразование компьютерной информации доступные для слабовидящих формы (укрупненный текст);
- в образовательном процессе используются социально-активные и рефлексивные методы обучения: кейс-метод, метод проектов, исследовательский метод, дискуссии в форме круглого стола, конференции, метод мозгового штурма.

Программа составлена в соответствии с требованиями ФГОС СПО по специальности 09.02.02 «Компьютерные сети».

Автор: Абросимова Е.В.

Рецензент: директор ООО "ЮМО-РТ" Ахметов М.Р.