Федеральное государственное бюджетное образовательное учреждение инклюзивного высшего образования

«Московский государственный гуманитарно-экономический университет»

Факультет Прикладной математики и информатики

Кафедра Информационных технологий и прикладной математики

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 041CD9B1001CAF77894D606F5F479EB1E9
Владелец: Сахарчук Елена Сергеевна
Действителен: с 26.09.2022 до 26.09.2023

УТВЕРЖДАЮ

И.о. Проректора по учебно-методической работе
Хакимов Р.М.
_____
«____»_____ 2021г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

образовательная программа направления подготовки
01.03.02 "Прикладная математика и информатика"
Б1.О.25 «Дисциплины (модули)», Обязательная часть

Профиль подготовки
Вычислительная математика и информационные технологии

Квалификация (степень) выпускника:
Бакалавр

Форма обучения: очная

Курс 3 семестр 5,6

Москва
2021

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению подготовки 01.03.02 «Прикладная математика и информатика (уровень бакалавриата)», утвержденного приказом Министерства образования и науки Российской Федерации № 9 от 10 января 2018 г. Зарегистрировано в Минюсте России 06 февраля 2018 г. №49937.

Составители рабочей программы: МГГЭУ, доцент кафедры информационных технологий и прикладной математики
место работы, занимаемая должность

подпись Белоглазов А.А «30» августа 2021 г.
Ф.И.О. Дата

Рецензент: МГГЭУ, профессор кафедры информационных технологий и прикладной математики
место работы, занимаемая должность

подпись Истомина Т.В. «30» августа 2021 г.
Ф.И.О. Дата

Рабочая программа утверждена на заседании кафедры Информационных технологий и прикладной математики (протокол № 2 от «30» августа 2021 г.)

Зав. кафедрой ИТиПМ подпись Митрофанов Е.П. «30» августа 2021 г.
Ф.И.О. Дата

СОГЛАСОВАНО
Начальник
учебного отдела
«30» августа 2021 г. подпись И.Г.Дмитриева
Дата Ф.И.О.

СОГЛАСОВАНО
Декан факультета ПМиИ
«30» августа 2021 г. подпись Е.В. Петрунина
Дата Ф.И.О.

СОГЛАСОВАНО
Заведующая библиотекой
«30» августа 2021 г. подпись В.А. Ахтырская
Дата Ф.И.О.

ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

1.1. Цель и задачи изучения учебной дисциплины (модуля)

Целью изучения дисциплины является подготовка студентов к освоению организационных, технических, алгоритмических и других методов и средств защиты компьютерной информации, ознакомление с законодательством и стандартами в этой области, с современными криптосистемами, изучение методов идентификации пользователей, борьбы с вирусами, изучение способов применения методов защиты информации при проектировании автоматизированных систем обработки информации и управления (АСОИУ).

Задачи:

- определение места дисциплины в предметном блоке, ее взаимосвязи с другими дисциплинами учебного плана специальности;
- раскрытие специфики защиты компьютерных сетей как объекта научного исследования;
- определение основных этапов и базовых концептуальных подходов к созданию систем защиты компьютерных сетей в рамках исторического развития отечественной и зарубежной науки;
- знакомство со способами и особенностями создания систем защиты компьютерных сетей на различных уровнях взаимодействия с окружением;
- приобретение студентами навыков аналитического и эмпирического исследования систем компьютерной защиты сетей;
- выработка целостного представления о различных аспектах строения и функционирования систем компьютерной защиты сетей на всех ее уровнях;
- рост навыков в сфере создания систем компьютерной защиты сетей и умения применять полученные знания на практике.

1.2. Требования к результатам освоения дисциплины

Изучение данной дисциплины направлено на формирование следующих компетенций:

Код и н содержание компетенции	**Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций**
ОПК-4. Способен решать задачи профессиональной деятельности с использованием существующих информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-4.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
	ОПК-4.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
	ОПК-4.3. Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.

1.3. Место дисциплины (модуля) в структуре образовательной программы направления подготовки01.03.02 Прикладная математика и информатика (бакалавриат)

Учебная дисциплина «Информационная безопасность» относится к основной части блока Б1. Изучение учебной дисциплины «Информационная безопасность» базируется на знаниях, умениях и навыках, полученных обучающимися при изучении предшествующих

курсов: «Вычислительные системы, сети и телекоммуникации», «Дискретная математика», «Основы информатики». Изучение учебной дисциплины «Информационная безопасность» необходимо для освоения таких дисциплин, как «Операционные системы», «Администрирование в информационных системах», «Криптография».

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1.Объем дисциплины и виды учебной работы в соответствии с формами обучения

Объем дисциплины «Информационная безопасность» составляет 7 зачетных единиц/ 252 часов:

Вид учебной работы	Всего, часов	Очная форма	
		Курс, часов	
	Очная форма	2 курс 3 сем.	2 курс 4 сем.
Аудиторная работа обучающихся с преподавателем (по видам учебных занятий), всего в том числе:	*64*	*32*	*32*
Лекции	24	12	12
Практические занятия	38	18	20
Лабораторные занятия			
Самостоятельная работа обучающихся	80	40	40
Промежуточная аттестация (подготовка и сдача), всего:			
Контрольная работа			
Курсовая работа			
Зачет	2	2	
Экзамен			36
Итого: Общая трудоемкость учебной дисциплины	**180/5**	72/2	108/3

2.2. Содержание дисциплины по темам (разделам)

№ раздела	Наименование раздела, тема	Содержание раздела	Форма текущего контроля
1.	Введение в информационную безопасность (ИБ)	Основные понятия. Анализ угроз. Проблемы безопасности компьютерных сетей. Политика безопасности. Основные составляющие политики безопасности. Нормативно-правовое обеспечение ИБ. Стандарты ИБ. Принципы защиты информационных систем (ИС).	Устный опрос
2.	Технологии защиты данных	Принципы криптозащиты. Криптографические алгоритмы. Симметричные и асимметричные системы шифрования. Технологии аутентификации. Биометрическая аутентификация.	Устный опрос, отчет по практической работе
3.	Технологии защиты вычислительных систем	Обеспечение безопасности операционных систем (ОС). Межсетевые экраны. Защита в виртуальных сетях VPN. Защита на уровнях модели OSI.	Устный опрос, отчет по практической работе
4.	Технологии обнаружения вторжений	Анализ защищенности. Обнаружение атак. Программные средства обнаружения вторжение. Защита удаленного доступа. Защита от вирусов и спама.	Устный опрос, отчет по практической работе
5.	Управление безопасностью	Задачи управления ИБ в информационных системах (ИС). Архитектура и функционирование систем управления ИБ в (ИС). Аудит и мониторинг безопасности (ИС).	Устный опрос, отчет по практической работе

		Обзор систем управления безопасностью.	

2.3. Разделы дисциплин и виды занятий

№ п/п	Наименование темы дисциплины	Лекционные занятия	Практические занятия	Самостоятельная работа	Всего часов	Формы текущего контроля успеваемости
1.	Введение в ИБ Основные понятия. Анализ угроз. Проблемы безопасности компьютерных сетей.	4		20	24	Устный опрос
2.	Технологии защиты данных. Принципы криптозащиты. Криптографические алгоритмы.	8	18	20	46	Устный опрос, отчет по практической работе
	Зачет		2		2	
	Итого:	12	20	40	72	
3.	Технологии защиты вычислительных систем.	4	6	10	20	Устный опрос, отчет по практической работе
4.	Технологии обнаружения вторжений. Анализ защищенности.	4	8	14	26	Устный опрос, отчет по практической работе
5.	Управление безопасностью. Задачи управления ИБ в информационных системах (ИС).	4	6	16	16	Устный опрос, отчет по практической работе
	Экзамен				36	
	Итого:	12	20	40	108	
	Всего:	24	40	80	180	

2.4. Планы теоретических (лекционных) занятий

№	Наименование тем лекций	Кол-во часов в 5,6 семестрах
	3 семестр	
РАЗДЕЛ 1. Введение в ИБ		
1.	Основные понятия. Анализ угроз. Проблемы безопасности компьютерных сетей. Политика безопасности. Основные составляющие политики безопасности. Нормативно-правовое обеспечение ИБ. Стандарты ИБ. Принципы защиты информационных систем (ИС).	4
РАЗДЕЛ 2. Технологии защиты данных		
1.	Принципы криптозащиты. Криптографические алгоритмы. Криптоанализ. Симметричные и асимметричные системы шифрования. Технологии электронно-цифровой подписи. Функции хэщирования. Технологии аутентификации. Биометрическая аутентификация.	8
	4 семестр	
РАЗДЕЛ 3. Технологии защиты вычислительных систем		
1.	Обеспечение безопасности операционных систем (ОС). Межсетевые экраны. Нормативно-правовое обеспечение. Сертификация и стандартизация. Защита в виртуальных сетях VPN. Защита на уровнях модели OSI.	4
РАЗДЕЛ 4. Технологии обнаружения вторжений		
1.	Анализ защищенности. Обнаружение атак. Защита удаленного доступа.	4

	Защита от вирусов и спама.	
РАЗДЕЛ 5. Управление безопасностью		
1.	Задачи управления ИБ в информационных системах (ИС). Архитектура и функционирование систем управления ИБ в (ИС). Аудит и мониторинг безопасности (ИС). Обзор систем управления безопасностью.	4

2.5. Планы практических (семинарских) занятий

№	Наименование тем практических занятий	Кол-во часов в 5,6 семестрах
3 семестр		
РАЗДЕЛ 2. Технологии защиты данных		
1.	Устройство и принцип работы шифровальной машины «Энигма». Методы защиты текстовой информации и их стойкость. Симметричные криптографический протоколы DES, 3DES, ГОСТ. Стандарт шифрования AESRijndael. Генерация простых чисел в ассиметричных алгоритмах шифрования. Электронная цифровая подпись. Изучение программы защиты информации PGP. Корректирующие коды.	18
4 семестр		
РАЗДЕЛ 3. Технологии защиты вычислительных систем		
1.	Механизмы защиты в ОС MicrosoftWindows. Захват и анализ сетевого трафика. Межсетевые экраны. Организация и защита VPN. Снифферы.	6
РАЗДЕЛ 4. Технологии обнаружения вторжений		
1.	Выявление сетевых атак путем анализа трафика. Системы обнаружения атак.Технологии терминального доступа.Аудит информационной безопасности компьютерных систем.Службы каталогов.	8
РАЗДЕЛ 5. Управление безопасностью		
1.	Создание и модификация виртуальной защищённой сети с помощью ПО.	6

2.6. Планы лабораторных работ – не предусмотрено.

2.7. Планы самостоятельной работы обучающегося по дисциплине (модулю)

№	Название разделов и тем	Виды самостоятельной работы	Трудо-емкость	Формируемые компетенции	Формы контроля
1.	Введение в информационную безопасность (ИБ). Политика безопасности. Нормативно-правовое обеспечение ИБ. Международные стандарты в сфере ИБ. Сравнение.	Работа с источниками	20	ОПК-4	Устный опрос
2.	Технологии защиты данных. Симметричные криптопротоколы. Сравнение.	Составление отчетов	20	ОПК-4	Устный опрос
3.	Технологии защиты вычислительных систем. Межсетевые экраны. Стандартизация и сертификация.	Работа с источниками	10	ОПК-4	Устный опрос
4.	Технологии обнаружения вторжений. Средство анализа сетевого трафика Wireshark. Сканирование сети.	Составление отчетов	14	ОПК-4	Устный опрос
5.	Управление безопасностью. Средство анализа сетевого	Работа с источниками	16	ОПК-3	Устный опрос

	трафика Wireshark. Сканирование сети. Настраивание параметров безопасности сети с использованием ПО Wireshark.	Составление отчетов			

3. ОСОБЕННОСТИ ОБУЧЕНИЯ ЛИЦ С ОВЗ (ПОДА)

Обучение лиц с ограниченными возможностями здоровья осуществляется с учетом индивидуальных психофизических особенностей, а для инвалидов также в соответствии с индивидуальной программой реабилитации инвалида.

Для получения обучающимися, имеющими ограниченные физические возможности, качественного образования должны выполняться следующие важные условия: обучающийся должен иметь возможность беспрепятственно посещать образовательное учреждение и использовать в своём обучении дистанционные образовательные технологии.

Для обучения и контроля обучающихся с нарушениями координации движений предусмотрено проведение тестирования с использованием компьютера.

Во время аудиторных занятий обязательно использование средств обеспечения наглядности учебного материала с помощью мультимедийного проектора. Скорость изложения материала должна учитывать ограниченные физические возможности студентов.

4. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое и информационное обеспечение дисциплины для организации самостоятельной работы студентов (содержит перечень основной литературы, дополнительной литературы, программного обеспечения и Интернет-ресурсы).

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Перечень основной литературы

1. Информационная безопасность : практи-кум / С. В. Озёрский, И. В. Попов, М. Е. Рычаго, Н. И. Улендеева. - Самара : Самар-ский юридический институт ФСИН Рос-сии, 2019. - 84 с. - ISBN 978-5-91612-276-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1094244

2. Баранова, Е. К. Информационная безопас-ность и защита информации : учебное по-собие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 336 с. — (Высшее об-разование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189326

3. Глинская, Е. В. Информационная безопас-ность конструкций ЭВМ и систем : учеб-ное пособие / Е.В. Глинская, Н.В. Чичва-рин. — Москва : ИНФРА-М, 2021. — 118 с. + Доп. материалы [Электронный ре-сурс]. — (Высшее образование: Бакалаври-ат). — DOI 10.12737/13571. - ISBN 978-5-16-010961-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1178152

4. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2021. — 400 с. — (Высшее об-разование). — DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1210523

5.1 Перечень дополнительной литературы

1. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2021. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/467370

2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2021. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/469235

3. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2021. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/473348

5.2 Электронные ресурсы

1. Электронная библиотека «Знаниум»: https://znanium.com/
2. Электронная библиотека «Юрайт»: https://urait.ru/
3. Научная электронная библиотека «Elibrary.ru»:https://www.elibrary.ru/defaultx.asp

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий	Перечень оборудования и технических средств обучения
1	Лекционная аудитория	Персональный компьютер, мультимедийный проектор
2	Компьютерный класс	Персональные компьютеры (IBMPC-совместимые) под управлением ОС MicrosoftWindows, компьютерная сеть, доступ в сеть Интернет. Интерактивная доска

7. ОЦЕНКА КОМПЕТЕНЦИЙ ПО ИЗУЧАЕМОЙ ДИСЦИПЛИНЕ

№	Критерии оценки	
	«незачтено»	**«зачтено»**
	ЗНАТЬ	
1	Студент не знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Не знает основные понятия ИБ, анализ угроз., проблемы безопасности компьютерных сетей. Политика безопасности. Стандарты ИБ. _ Не знает принципы защиты информационных систем (ИС), криптографических методы защиты информации.	Студент знает, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.Знает основные понятия ИБ, анализ угроз, проблемы безопасности компьютерных сетей. Политика безопасности. Стандарты ИБ. Показывает глубокое знание и понимание принципов защиты информационных систем (ИС), криптографических методов защиты информации, знание стандартов шифрования электронная цифровая подписи,
	УМЕТЬ	
2	Студент не умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Студент испытывает затруднения при анализе угроз ИБ, политики безопасности ИС. Студент не умеетсамостоятельно разрабатывать политику безопасности ИС	Студент умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Студент умеет анализировать проблем безопасности компьютерных сетей. Политики безопасности. Стандарты ИБ. Студент умеет самостоятельно разрабатывать политику безопасности ИС,
	ВЛАДЕТЬ	
3	Студент не владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности. Студент не владеет навыками концептуально-понятийным	Студент владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности. Студент владеет концептуально-понятийным аппаратом,

	аппаратом, научным языком и терминологиейкриптографических методов защиты текстовой информациистандартов шифрования, ЭЦП.	научным языком и терминологиейкриптографических методов защиты текстовой информации. Стандартов шифрования, ЭЦП.Студент владеет знаниями всего изученного материала, владеет навыками

№	Критерии оценки			
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
ЗНАТЬ				
1	Студент не знаетпринципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Отсутствуют знания и понимание основ и методов обеспечения безопасности компьютерных сетей, политики безопасности, стандарты ИБ. принципы защиты информационных систем_	Студент усвоил принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.Показывает поверхностное знание методов обеспечения безопасности компьютерных сетей, политики безопасности, стандарты ИБ. принципы защиты информационных систем	Знает основныеметоды и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Показывает знание методов обеспечения безопасности компьютерных сетей, политики безопасности, стандарты ИБ, принципы защиты информационных систем.	Студент знает, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Показывает глубокое знание и понимание основ и методов обеспечения безопасности компьютерных сетей, политики безопасности, стандарты ИБ. принципы защиты информационных систем, криптографические методы защиты информации. Знает архитектуру и функционирование систем управления ИБ в (ИС).
УМЕТЬ				

2	Студент не умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.Не умеет проводить анализ защищенности ИС, обнаружение атак,защиту удаленного доступа, защиту от вирусов и спама.	Студент испытывает затрудненияпри решении стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Студент испытывает затруднения при проведении анализа защищенности ИС, обнаружении атак,защите удаленного доступа, защите от вирусов и спама	Студент умеет самостоятельнорешать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.Студент может проводить анализ защищенности ИС, обнаружение атак, зашиту от вирусов и спама.	Студент умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Умеет проводить анализ защищенности ИС, обнаружение атак,защиту удаленного доступа, защиту от вирусов и спама.
ВЛАДЕТЬ				
3	Студент не владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности. Студент не владеет навыками обеспечение безопасности ОС, управления ИБ в информационных системах (ИС). Не владеет знаниями об аудите и мониторинге безопасности (ИС). навыками управления	Студент частично владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.Студент владеет основными навыками обеспечение безопасности ОС, управления ИБ в информационных системах (ИС). Владеет знаниями об аудите и мониторинге	Студент в большей степени владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности. Студент владеет знаниями всего изученного материала, владеет навыками обеспечение безопасности ОС, управления ИБ в информационных	Студент владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности. Студент владеет навыками обеспечение безопасности ОС, управления ИБ в информационных системах (ИС).Владеет знаниями об аудите и мониторинге

	безопасностью ИС, выявления сетевых атак путем анализа трафика., аудита информационной безопасности компьютерных систем	безопасности (ИС).	системах (ИС). (ИС). Навыками управления безопасностью ИС, выявления сетевых атак путем анализа трафика. Испытывает затруднения при проведении аудита информационной безопасности компьютерных систем	безопасности (ИС). Навыками управления безопасностью ИС, выявления сетевых атак путем анализа трафика., аудитаинформационной безопасности компьютерных систем
	Компетенция или ее часть не сформирована	Компетенция или ее часть сформирована на базовом уровне	Компетенция или ее часть сформирована на среднем уровне	Компетенция или ее часть сформирована на высоком уровне

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

8.1. Интерактивные образовательные технологии, используемые в аудиторных занятиях и самостоятельной работе обучающихся – не предусмотрены.

9. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

9.1.Организация входного, текущего и промежуточного контроля обучения

Входное тестирование – не предусмотрено.

Текущий контроль – устный опрос, защита по практическим работам.

Промежуточная аттестация – зачет, экзамен.

9.2. Тематика рефератов, проектов, творческих заданий, эссе и т.п.

Не предусмотрено.

9.3. Курсовая работа

Не предусмотрено.

9.4. Вопросы к зачету

1. Основные понятия защиты информации и информационной безопасности
2. Анализ угроз информационной безопасности
3. Проблемы безопасности IP-сетей
4. Угрозы и уязвимости проводных корпоративных сетей
5. Угрозы и уязвимости беспроводных сетей
6. Способы обеспечения информационной безопасности
7. Основные понятия политики безопасности
8. Структура политики безопасности организации. Базовая политика безопасности. Специализированные политики безопасности. Процедуры безопасности
9. Роль стандартов информационной безопасности
10. Стандарты ISO/IEC 17799:2002 (BS 7799:2000)
11. Стандарт BSI
12. Международный стандарт ISO 15408 «Общие критерии безопасности информационных технологий»
13. Стандарты для беспроводных сетей
14. Стандарты информационной безопасности в Интернете
15. Отечественные стандарты безопасности информационных технологий
16. Основные понятия криптографической защиты информации
17. Симметричные криптосистемы шифрования
18. Асимметричные криптосистемы шифрования
19. Комбинированная криптосистема шифрования
20. Электронная цифровая подпись и функция хэширования
21. Управление криптоключами
22. Классификация криптографических алгоритмов
23. Симметричные алгоритмы шифрования. Блочные алгоритмы шифрования данных
24. Асимметричные криптоалгоритмы. Алгоритм шифрования RSA.Алгоритмы цифровой подписи
25. Аутентификация, авторизация и администрирование действий пользователей
26. Методы аутентификации, использующиепароли и PIN-коды
27. Строгая аутентификация

28. Биометрическая аутентификация пользователя
29. Угрозы безопасности ОС
30. Понятие защищенной ОС
31. Основные функции подсистемы защиты ОС
32. Идентификация, аутентификация и авторизация субъектов доступа
33. Разграничение доступа к объектам ОС
34. Аудит безопасности в ОС.

9.5. Вопросы к экзамену

1. Основные понятия защиты информации и информационной безопасности
2. Анализ угроз информационной безопасности
3. Анализ угроз сетевой безопасности.
4. Способы обеспечения информационной безопасности
5. Основные понятия политики безопасности.
6. Структура политики безопасности организации. Процедуры безопасности
7. Разработка политики безопасности.
8. Стандарты информационной безопасности
9. Основные понятия криптографической защиты информации
10. Симметричные криптосистемы шифрования
11. Асимметричные криптосистемы шифрования
12. Комбинированная криптосистема шифрования
13. Электронная цифровая подпись и функция хэширования
14. Управление криптоключами
15. Аутентификация, авторизация и администрирование действий пользователей
16. Безопасность КИС.
17. Безопасность облачных вычислений.
18. Обеспечение безопасности ОС.
19. Функции межсетевых экранов
20. Особенности функционирования
21. Схемы сетевой защиты на базе МЭ
22. Концепция построения виртуальных защищенных сетей VPN
23. VPN-решения для построения защищенных сетей
24. Протоколы формирования защищенныхканалов на канальном уровне
25. Протоколы формирования защищенныхканалов на сеансовом уровне
26. Защита беспроводных сетей
27. Архитектура средств безопасности IPSec. Защита передаваемых данных с помощьюпротоколов AH и ESP
28. Протокол управления криптоключами IKE
29. Основные схемы применения IPSec. Преимущества средств безопасности IPSec
30. Управление идентификацией и доступом
31. Организация защищенного удаленного доступа. Централизованный контрольудаленного доступа
32. Управление доступом по схеме однократноговхода с авторизацией Single Sign-On (SSO)
33. Протокол Kerberos
34. Инфраструктура управления открытымиключами PKI
35. Технология анализа защищенности
36. Технологии обнаружения атак
37. Компьютерные вирусы и проблемы антивирусной защиты.
38. Концепция адаптивного управления безопасностью

9.6. Контроль освоения компетенций

Вид контроля	**Контролируемые темы (разделы)**	**Компетенции, компоненты которых контролируются**
Устный опрос	*1,2,3,4,5*	*ОПК-4*
Отчет по практической работе	*2,3,4,5*	*ОПК-4*

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Номер и дата протокола заседания кафедры	Перечень измененных пунктов	Подпись заведующего кафедрой