Федеральное государственное бюджетное образовательное учреждение инклюзивного высшего образования
«Московский государственный гуманитарно-экономический университет»
Факультет прикладной математики информатики
Кафедра информационных технологий и прикладной математики

УТВЕРЖДАЮ

Проректор по организации образовательной деятельности

Ковалева М.А. _____
«24» августа 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ ПЕДАГОГА

образовательная программа направления подготовки
44.03.02 Психолого-педагогическое образование
блок Б1.В.ДВ.11.01 «Дисциплины (модули)», часть, формируемая участниками образовательных отношений

Профиль подготовки

«Психология и педагогика инклюзивного образования»

Квалификация (степень) выпускника
Бакалавр

Форма обучения очная, заочная

Курс 2 семестр 4

Москва
2020

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего профессионального образования направления (специальности) Психолого-педагогическое образование, утвержденного приказом Министерства образования и науки Российской Федерации № 122 от 22.02.2018

Зарегистрировано в Минюсте России « 15 » марта 2018 г. № 50364

Составители рабочей программы: доцент кафедра информационных технологий и прикладной математики старший преподаватель кафедры информац. технологий и прикладной математики
место работы, занимаемая должность

подпись Труб Т.В. /Ф.И.О. Дата 24 августа 2020 г.

Рецензент: кандидат физико-матем. наук, доцент
место работы, занимаемая должность

подпись Нецубидзе Л.В. Ф.И.О. Дата 24 августа 2020 г.

Рабочая программа утверждена на заседании кафедры информационных технологий и прикладной математики

(протокол № 1 от « 24 » августа 20 20 г.)

Заведующий кафедрой подпись Петрунина Е.В. Ф.И.О. 24.08 Дата 2020 г.

СОГЛАСОВАНО
Начальник
учебного отдела

« 24 » августа 2020 г. (дата) (подпись) Дмитриева И. Г. (Ф.И.О.)

СОГЛАСОВАНО
Декан
факультета

« 24 » августа 2020 г. (дата) (подпись) Петрунина Е. В. (Ф.И.О.)

СОГЛАСОВАНО
Заведующий
библиотекой

« 24 » августа 2020 г. (дата) (подпись) Ахтырская В.А. (Ф.И.О.)

1. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

1.1. Цель и задачи изучения учебной дисциплины (модуля)

Целью изучения дисциплины «Информационная безопасность в профессиональной деятельности педагога» 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:

- раскрытие основных принципов и методов построения систем информационной безопасности;
- определение основных этапов и базовых концептуальных подходов к созданию систем информационной в рамках исторического развития отечественной и зарубежной науки;
- ознакомление с нормативно-правовыми информационной безопасности автоматизированных систем обработки информации;
- ознакомление 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.

1.2. Требования к результатам освоения дисциплины

Изучение данной дисциплины направлено на формирование следующих компетенций:

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**
УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1. Знает необходимые для осуществления профессиональной деятельности правовые нормы и методологические основы принятия управленческого решения.
	УК-2.2. Умеет анализировать альтернативные варианты решений для достижения намеченных результатов; разрабатывать план, определять целевые этапы и основные направления работ.
	УК-2.3. Владеет методиками разработки цели и задач проекта; методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах.

1.3. Место дисциплины (модуля) в структуре образовательной программы направления подготовки 44.03.02. «Психолого-педагогическое образования (уровень бакалавриата)».

Учебная дисциплина «Информационная безопасность в профессиональной деятельности педагога» относится к части, формируемой участниками образовательных отношений блока Б1. Изучение учебной дисциплины «Информационная безопасность в профессиональной деятельности педагога» базируется на знаниях, умениях и навыках, полученных обучающимися при изучении предшествующих курсов: «Математика», «Современные информационные

технологии», «Информационные системы и базы данных по психологии и педагогике». Изучение учебной дисциплины «Информационная безопасность в профессиональной деятельности педагога» необходимо для освоения таких дисциплин, как «Теория и технологии обучения детей младшего школьного возраста», «Теория и технологии организации образовательной деятельности в дошкольном образовательном учреждении» и для подготовки выпускной квалификационной работы.

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

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

Объем дисциплины «Информационная безопасность в профессиональной деятельности педагога» составляет 2 зачетных единиц/ 72 часов:

Очная форма

Вид учебной работы	Всего, часов	Очная форма
		Курс, часов
		2 курс 4 сем.
Аудиторная работа обучающихся с преподавателем (по видам учебных занятий), всего в том числе:	*36*	*36*
Лекции	12	12
Практические занятия	24	24
Лабораторные занятия		
Самостоятельная работа обучающихся	36	36
Промежуточная аттестация (подготовка и сдача), всего:		
Контрольная работа		
Курсовая работа		
Зачет	2	2
Экзамен		
Итого: Общая трудоемкость учебной дисциплины (в часах, зачетных единицах)	**72/2**	72/2

Заочная форма

Вид учебной работы	Всего, часов	Заочная форма
		Курс, часов
Аудиторная работа обучающихся с преподавателем (по видам учебных занятий), всего в том числе:	*6*	*6*
Лекции	2	2
Практические занятия	2	2
Лабораторные занятия		
Самостоятельная работа обучающихся	62	62
Промежуточная аттестация (подготовка и сдача), всего:		
Контрольная работа		
Курсовая работа		
Зачет	4	4
Экзамен		
Итого: Общая трудоемкость учебной дисциплины (в часах, зачетных единицах)	**72/2**	72/2

2.2. Содержание дисциплины по темам (разделам)

№ раздела	Наименование раздела, тема	Содержание раздела	Формируемые компетенции (индекс)
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).	УК-2
2.	Технологии защиты данных	Принципы криптозащиты. Криптографические алгоритмы. Симметричные и асимметричные системы шифрования. Технологии аутентификации. Биометрическая аутентификация.	УК-2
3.	Технологии защиты вычислительных систем	Обеспечение безопасности операционных систем (ОС). Межсетевые экраны. Защита в виртуальных сетях VPN. Защита на уровнях модели OSI.	УК-2
4.	Технологии обнаружения вторжений	Анализ защищенности. Обнаружение атак. Программные средства обнаружения вторжение. Защита удаленного доступа. Защита от вирусов и спама.	УК-2
5.	Управление безопасностью	Задачи управления ИБ в информационных системах (ИС). Архитектура и функционирование систем управления ИБ в (ИС). Аудит и мониторинг безопасности (ИС). Обзор систем управления безопасностью.	УК-2

2.3. Разделы дисциплин и виды лекционных занятий
Очная форма

№ п/п	Наименование темы дисциплины	Лекционные занятия	Практические занятия	Самостоятельная работа	Всего часов	Формы текущего контроля успеваемости
1.	Введение в информационную безопасность (ИБ).	4	2	6	12	Устный опрос, тестирование
2.	Технологии защиты данных.	2	8	6	16	Устный опрос, тестирование
3.	Технологии защиты вычислительных систем.	2	4	8	14	Устный опрос, тестирование
4.	Технологии обнаружения вторжений.	2	6	8	16	Устный опрос, тестирование
5.	Управление безопасностью.	2	2	8	12	Устный опрос, тестирование
	Зачет		2		2	
	Итого:	12	24	36	72	

Всего:	12	24	36	72	

Заочная форма

№ п/п	Наименование темы дисциплины	Лекционные занятия	Практические занятия	Самостоятельная работа	Всего часов	Формы текущего контроля успеваемости
1.	Введение в информационную безопасность (ИБ).	0,5		6	6,5	Устный опрос, тестирование
2.	Технологии защиты данных.	0,5	1	6	7,5	Устный опрос, тестирование
3.	Технологии защиты вычислительных систем.	0,5	1	6	7,5	Устный опрос, тестирование
4.	Технологии обнаружения вторжений.	0,5	1,5	7	9	Устный опрос, тестирование
5.	Управление безопасностью.		0,5	7	7,5	Устный опрос, тестирование
Зачет		2	4	62	4	
Итого:					72	
Всего:					72	

2.4. Планы теоретических (лекционных) занятий

Очная форма

№	Наименование тем лекций	Кол-во часов в 4 семестре
4 семестр		
РАЗДЕЛ 1. Введение в ИБ		
1.	Основные понятия. Анализ угроз. Проблемы безопасности компьютерных сетей. Политика безопасности. Основные составляющие политики безопасности.	2
2.	Нормативно-правовое обеспечение ИБ. Стандарты ИБ. Принципы защиты информационных систем (ИС).	2
РАЗДЕЛ 2. Технологии защиты данных		
1.	Принципы криптозащиты. Криптографические алгоритмы. Криптоанализ. Симметричные и асимметричные системы шифрования. Технологии электронно-цифровой подписи. Функции хэширования. Технологии аутентификации. Биометрическая аутентификация.	2
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.	2
РАЗДЕЛ 4. Технологии обнаружения вторжений		
1.	Анализ защищенности. Обнаружение атак. Защита удаленного доступа. Защита от вирусов и спама.	2
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.	2

заочная форма

№	Наименование тем лекций	Кол-во часов
4 семестр		
РАЗДЕЛ 1. Введение в ИБ		
1.	Основные понятия. Анализ угроз. Проблемы безопасности компьютерных сетей. Политика безопасности. Основные составляющие политики безопасности.	0,5
2.	Нормативно-правовое обеспечение ИБ. Стандарты ИБ. Принципы защиты информационных систем (ИС).	
РАЗДЕЛ 2. Технологии защиты данных		
1.	Принципы криптозащиты. Криптографические алгоритмы. Криптоанализ. Симметричные и асимметричные системы шифрования. Технологии электронно-цифровой подписи. Функции хэширования. Технологии аутентификации. Биометрическая аутентификация.	0,5
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.	0,5
РАЗДЕЛ 4. Технологии обнаружения вторжений		
1.	Анализ защищенности. Обнаружение атак. Защита удаленного доступа. Защита от вирусов и спама.	0,5
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.	

2.5. Планы практических (семинарских) занятий

Очная форма

№	Наименование тем практических занятий	Кол-во часов в 4 семестре
4 семестр		
РАЗДЕЛ 1. Введение в ИБ		
1.	Политика безопасности. Основные составляющие политики безопасности	2
РАЗДЕЛ 2. Технологии защиты данных		
1.	Устройство и принцип работы шифровальной машины «Энигма». Методы защиты текстовой информации и их стойкость.	2
2.	Симметричные криптографический протоколы DES, 3DES, ГОСТ. Стандарт шифрования AES Rijndael.	2
3.	Генерация простых чисел в ассиметричных алгоритмах шифрования. Электронная цифровая подпись.	2
4.	Изучение программы защиты информации PGP. Корректирующие коды.	2
РАЗДЕЛ 3. Технологии защиты вычислительных систем		
1.	Механизмы защиты в ОС Microsoft Windows. Захват и анализ сетевого трафика.	2

2.	Межсетевые экраны. Организация и защита VPN. Снифферы.	2
РАЗДЕЛ 4. Технологии обнаружения вторжений		
1.	Выявление сетевых атак путем анализа трафика. Системы обнаружения атак.	2
2.	Технологии терминального доступа	2
3.	Аудит информационной безопасности компьютерных систем. Службы каталогов.	2
РАЗДЕЛ 5. Управление безопасностью		
1.	Создание и модификация виртуальной защищѐнной сети с помощью ПО.	2

Заочная форма

№	Наименование тем практических занятий	Кол-во часов
4 семестр		
РАЗДЕЛ 1. Введение в ИБ		
1.	Политика безопасности. Основные составляющие политики безопасности	
РАЗДЕЛ 2. Технологии защиты данных		
1.	Устройство и принцип работы шифровальной машины «Энигма». Методы защиты текстовой информации и их стойкость.	
2.	Симметричные криптографический протоколы DES, 3DES, ГОСТ. Стандарт шифрования AES Rijndael.	
3.	Генерация простых чисел в ассиметричных алгоритмах шифрования. Электронная цифровая подпись.	0,5
4.	Изучение программы защиты информации PGP. Корректирующие коды.	0,5
РАЗДЕЛ 3. Технологии защиты вычислительных систем		
1.	Механизмы защиты в ОС Microsoft Windows. Захват и анализ сетевого трафика.	0,5
2.	Межсетевые экраны. Организация и защита VPN. Снифферы.	0,5
РАЗДЕЛ 4. Технологии обнаружения вторжений		
1.	Выявление сетевых атак путем анализа трафика. Системы обнаружения атак.	0,5
2.	Технологии терминального доступа	0,5
3.	Аудит информационной безопасности компьютерных систем. Службы каталогов.	0,5
РАЗДЕЛ 5. Управление безопасностью		
1.	Создание и модификация виртуальной защищѐнной сети с помощью ПО.	0,5

2.6. Планы лабораторных работ – не предусмотрено.

2.7. Планы самостоятельной работы обучающегося по дисциплине (модулю)

Очная форма

№	Название разделов и тем	Виды самостоятельной работы	Трудоемкость	Формируемые компетенции	Формы контроля
1.	Введение в информационную безопасность (ИБ).	Сравнение международных стандартов в сфере ИБ.	8	УК-2	Устный опрос, тестирование
2.	Технологии защиты данных.	Сравнение симметричных криптопротоколов.	8	УК-2	Устный опрос, тестирование

3.	Технологии защиты вычислительных систем.	Технологии защиты вычислительных систем. Межсетевые экраны.	8	УК-2	Устный опрос, тестирование
4.	Технологии обнаружения вторжений.	Средство анализа сетевого трафика Wireshark.	8	УК-2	Устный опрос, тестирование
5.	Управление безопасностью.	Управление безопасностью. Сканирование сети.	8	УК-2	Устный опрос, тестирование

Заочная форма

№	Название разделов и тем	Виды самостоятельной работы	Трудоемкость	Формируемые компетенции	Формы контроля
1.	Введение в информационную безопасность (ИБ).	Сравнение международных стандартов в сфере ИБ.	6,5	УК-2	Устный опрос, тестирование
2.	Технологии защиты данных.	Сравнение симметричных криптопротоколов.	7,5	УК-2	Устный опрос, тестирование
3.	Технологии защиты вычислительных систем.	Технологии защиты вычислительных систем. Межсетевые экраны.	7,5	УК-2	Устный опрос, тестирование
4.	Технологии обнаружения вторжений.	Средство анализа сетевого трафика Wireshark.	9	УК-2	Устный опрос, тестирование
5.	Управление безопасностью.	Управление безопасностью. Сканирование сети.	7,5	УК-2	Устный опрос, тестирование

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 своѐм 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 конструкций ЭВМ и систем : учеб. пособие / Е.В. Глинская, Н.В. Чичварин. — Москва : ИНФРА-М, 2019. — 118 с. + Доп. материалы [Электронный ресурс; Режим доступа: https://new.znanium.com]. — (Высшее образование: Бакалавриат). — www.dx.doi.org/10.12737/13571. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/991792.

2. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с. — (Университеты России). — ISBN 978-5-534-00258-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/434171.

5.2 Перечень дополнительной литературы

1. Защита информации : учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - Москва : РИОР : ИНФРА-М, 2018. - 392 с. - (Высшее образование: Бакалавриат; Магистратура). — https://doi.org/10.12737/4868. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/937469.

2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва :

Издательство Юрайт, 2019. — 325 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/432966.

3. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для бакалавриата и магистратуры / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2019. — 342 с. — (Бакалавр и магистр. Модуль). — ISBN 978-5-534-05142-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/441287.

5.3 Программное обеспечение

1. Сетевой компьютерный класс, оснащенный современной техникой
2. Офисный программный пакет (например, Microsoft Office 2003 или более поздних версий).
3. Web-браузер Mozilla Firefox или Google Chrome
4. Экран для проектора

5.4 Электронные ресурсы

1. Открытый ПП SiLab.
2. Национальный открытый Университет «ИНТУИТ» www.intuit.ru
3. Энциклопедия Кругосвет. Универсальная научно-популярная онлайн-энциклопедия. www.krugosvet.ru
4. Электронная библиотека: https://biblio-online.ru/
5. Электронная библиотека: https://new.znanium.com/

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 (IBM PC-совместимые) под управлением ОС Microsoft Windows, компьютерная сеть, доступ в сеть Интернет. Интерактивная доска

7. ОЦЕНКА КОМПЕТЕНЦИЙ ПО ИЗУЧАЕМОЙ ДИСЦИПЛИНЕ

№	Критерии оценки	
	«незачтено»	**«зачтено»**
	ЗНАТЬ	
1	Студент не способен самостоятельно выделять главные положения в изученном материале дисциплины. Не знает правовые основы защиты компьютерной информации; организационные, технические и программные методы защиты информации в АСОИУ; стандарты, модели и методы шифрования; методы идентификации пользователей; методы защиты программ от вирусов и вредоносных программ; требования к системам информационной защиты АСОИУ и компьютерных сетей.	Студент самостоятельно выделяет главные положения в изученном материале. Показывает глубокое знание и понимание правовых основ защиты компьютерной информации; организационных, технических и программных методов защиты информации в АСОИУ; стандартов, моделей и методов шифрования; методов идентификации пользователей; методов защиты программ от вирусов и вредоносных программ; требований к системам информационной защиты АСОИУ и компьютерных сетей.
	УМЕТЬ	
2	Студент испытывает затруднения при применении методов защиты компьютерных сетей при проектировании АСОИУ в различных предметных областях.	Студент умеет самостоятельно применять методы защиты компьютерных сетей при проектировании АСОИУ в различных предметных областях.
	ВЛАДЕТЬ	
3	Студент не владеет навыками использования информации о роли и месте защиты информации в компьютерных сетях; навыками использования информации о направлениях и перспективах развития защиты информации.	Студент владеет знаниями всего изученного материала, концептуально-понятийным аппаратом, научным языком и терминологией. Студент владеет навыками использования информации о роли и месте защиты информации в компьютерных сетях; навыками использования информации о направлениях и перспективах развития защиты информации.
	Компетенция или ее часть не сформирована.	Компетенция или ее часть сформирована на базовом, среднем или 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, тестирование.
Промежуточная аттестация – зачет.

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. 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 защищенных каналов на канальном уровне
25. Протоколы формирования защищенных каналов на сеансовом уровне
26. Защита беспроводных сетей
27. Архитектура средств безопасности IPSec. Защита передаваемых данных с помощью протоколов 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 контроль удаленного доступа
32. Управление доступом по схеме однократного входа с авторизацией Single Sign-On (SSO)
33. Протокол Kerberos
34. Инфраструктура управления открытыми ключами PKI
35. Технология анализа защищенности
36. Технологии обнаружения атак
37. Компьютерные вирусы и проблемы антивирусной защиты.
38. Концепция адаптивного управления безопасностью

9.5. Вопросы к экзамену

Не предусмотрено.

9.6. Контроль освоения компетенций

Вид контроля	**Контролируемые темы (разделы)**	**Компетенции, компоненты которых контролируются**
Устный опрос	*1,2,3,4,5*	*УК-2*
Тестирование	*1,2,3,4,5*	*УК-2*

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

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