ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ИНКЛЮЗИВНОГО ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО - ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет Прикладной математики и информатики
Кафедра Прикладной математики и информатики по областям

УТВЕРЖДАЮ

И.о. проректора по учебно-методической работе
Хакимов Р.М.

«30»августа 2021г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

образовательная программа направления подготовки
09.04.03 "Прикладная информатика"
Блок Б1.В.02 «Дисциплины (модули)», часть формируемая участниками образовательных отношений

Профиль подготовки
Интеллектуальные биоинформационные технологии

Квалификация (степень) выпускника

Магистр

Форма обучения: очная

Курс 1 семестр 1

Москва
2021

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.04.03 «Прикладная информатика (уровень магистратуры)», утвержденного приказом Министерства образования и науки Российской Федерации № 916 от 19 сентября 2017 г. Зарегистрировано в Минюсте России 10 октября 2017 г. №48495.

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. _____ И.Г.Дмитриева

Дата подпись Ф.И.О.

СОГЛАСОВАНО
Декан факультета ПМиИ

«30» августа 2021 г. Е.В. Петрунина

Дата подпись Ф.И.О.

СОГЛАСОВАНО
Заведующая библиотекой

«30» августа 2021 г. _____ В.А. Ахтырская

Дата подпись Ф.И.О.

1. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

1.1. Цели и задачи изучения дисциплины

Цели освоения дисциплины:

- освоение общих принципов, методов и механизмов обеспечения компьютерной безопасности;
- изучение политики и моделей безопасности информации в компьютерных системах.

Задачи освоения дисциплины:

- обобщение базовых знаний по субъектно-объектной модели компьютерной системы в механизмах и процессах коллективного доступа к информационным ресурсам;
- изучение понятия информационной безопасности, её цели, механизмы, инструментарий и основные направления;
- изучение моделей дискреционного доступа, мандатного доступа, моделей разграничения доступа на основе функционально-ролевых отношений;
- изучение источников угроз информационной безопасности, изложение основных принципов защиты компьютерной информации и их оценки.

1.2. Требования к результатам освоения дисциплины

Изучение данной дисциплины направлено на формирование следующих компетенций:

Код и содержание компетенции	**Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций**
ПК-6 Способен применять современные методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания ИС	ПК-6.1 Знает различные методы решения задач при создании экономических информационных систем; методы проектирования автоматизированных и информационных систем для решения прикладных задач; информационные технологии, применяемые на этапах разработки, производства, испытаний и эксплуатации продукции.
	ПК-6.2 Умеет осуществлять выбор способа представления информации в соответствии с поставленной задачей; видеть и формулировать проблему информационной безопасности и надежности, ее анализировать, подбирать средства и методы для ее решения и ликвидации; использовать программные средства, применяемые на этапах разработки, производства, испытаний и эксплуатации продукции.
	ПК-6.3 Владеет навыками применения типовых подходов, применяемых при анализе, планировании и оперативном управлении деятельностью промышленного предприятия; навыками исследования применения различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций на основе приобретенных знаний и умений и их применения в нетипичных ситуациях.

1.3. Место дисциплины (модуля) в структуре образовательной программы направления подготовки 09.04.03 Прикладная информатика (уровень магистратуры).

Учебная дисциплина «Теоретические основы компьютерной безопасности» относится к части, формируемой участниками образовательных отношений блока «Дисциплин (модулей)» блока Б1. Изучение этой учебной дисциплины базируется на знаниях, умениях и навыках, полученных обучающимися при изучении предшествующих курсов: «Математические инструментальные методы и модели систем поддержки принятия решений», «Современные технологии разработки программного обеспечения», «Стандартизация и лицензирование в сфере биоинформационных технологий». Изучение учебной дисциплины необходимо для освоения такой дисциплины как «Современные методы разработки биомедицинских систем», прохождения производственной и преддипломной практик.

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

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

Объем дисциплины «Теоретические основы компьютерной безопасности» составляет 4 з.е./144 часа:

Вид учебной работы	Всего, часов	Очная форма
		Курс, часов
	Очная форма	1 курс 1 семестр
Аудиторная работа обучающихся с преподавателем (по видам учебных занятий), всего в том числе:	**40**	**40**
Лекции	12	12
В том числе, практическая подготовка (ЛПП)		
Практические занятия	28	28
В том числе, практическая подготовка (ПЗПП)	**8**	**8**
Лабораторные занятия		
В том числе, практическая подготовка (ЛРПП)		
Самостоятельная работа обучающихся	**68**	**68**
В том числе, практическая подготовка (СРПП)	**20**	**20**
Промежуточная аттестация (подготовка и сдача), всего:		
Контрольная работа		
Курсовая работа		
Зачет		
Экзамен	**36**	**36**
Итого: Общая трудоемкость учебной дисциплины (в часах, зачетных единицах)	144 часов (4з.е.)	144 часов (4з.е.)

2.2. Содержание дисциплины по темам (разделам)

№ п/п	Наименование раздела (темы)	Содержание раздела (тематика занятий)	Формируемые компетенции (индекс)
1.	Раздел 1. Основные понятия теории компьютерной безопасности.	Основные понятия теории компьютерной безопасности. Язык. Объекты. Субъекты. Доступ. Ценность информации. Аддитивная модель. Порядковая шкала. Решетка ценности. Анализ угроз информацион-ной безопасности. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы. Структура теории компьютерной безопасности. Основные уровни защиты информации. Защита машинных носителей информации и средств взаимодействия. Защита представления информации. Защита содержания информации. Основные виды атак на автоматизированные системы обработки информации. Классификация основных атак и вредоносных программ.	ПК-6
2.	Раздел 2. Политики безопасности	Понятие политики безопасности. Политика (стратегия) безопасности. Дискреционная политика разграничения доступа. Мандатная (полномочная) политика разграничения доступа. Политика безопасности информационных потоков. Политика ролевого разграничения доступа. Политика изолированной программной среды. Разработка и реализация политики безопасности. Модели безопасности. Описание систем защиты с помощью матрицы доступа.	ПК-6
3.	Раздел 3. Дискреционная политика разграничения доступа	Модель Харрисона-Руззо-Ульмана. Модель распространения прав доступа Take-Grant. Разрешимость проблемы безопасности. Расширенная модель Take-Grant. Анализ информационных каналов.	ПК-6
4.	Раздел 4. Мандатная политика разграничения доступа	Классическая модель Белла-ЛаПадулы. Свойства безопасности системы в классической модели Белла-ЛаПадула. Базовая теорема безопасности в классической модели Белла-ЛаПадула. Эквивалентные подходы к определению безопасности модели Белла-Лападулы. Политика low-watermark в модели Белла-ЛаПадула. Условия и результаты	ПК-6

		выполнения операций при реализации политики low-watermark в модели Белла-ЛаПадула. Безопасность переходов в классической модели Белла-ЛаПадула. Функция переходов и ее безопасность в смысле администрирования в классической модели Белла-ЛаПадула. Модель мандатной политики целостности информации Биба.	
5.	Раздел 5. Активный аудит моделей безопасности	Активный аудит. Общая архитектура системы и методы анализа. Сигнатурный анализ. Теорема Клини. Статистический анализ. Алгоритм NIDES. Состоятельность оценки числа ребер случайного графа. Модели безопасности в базах данных. Понятие реляционной базы данных и реляционных операторов. Декомпозиция и восстановление многоуровневой базы данных. Теорема Эрдёша-Реньи.	ПК-6
6.	Раздел 6. Модель систем военных сообщений	Общие положения и основные понятия модели систем военных сообщений. Модель CBC (MMS). Неформальное описание модели систем военных сообщений. Формальное описание модели систем военных сообщений. Безопасное состояние в модели систем военных сообщений. Безопасность переходов в модели систем военных сообщений. Определения смыслов безопасности функции переходов в модели систем военных сообщений. Базовая теорема безопасности (BST) в модели систем военных сообщений. Теорема о безопасности системы в модели систем военных сообщений.	ПК-6

2.3. Разделы дисциплин и виды занятий

Очная форма обучения

№ раз-дела	Наименование темы дисциплины	Аудиторная работа				Внеаудиторная работа		Объем в часах	
		Л	в том числе ЛПП	ПЗ	в том числе ПЗПП	СР	в том числе СРПП	Всего	в том числе ПП
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1.	Раздел 1. Основные понятия теории компьютерной безопасности.	2		4		8	2	14	
2.	Раздел 2. Политики безопасности	2		4		12	2	18	
3.	Раздел 3. Дискреционная политика разграничения доступа	2		4	2	12	4	18	
4.	Раздел 4. Мандатная политика разграничения доступа	2		4	2	12	4	18	
5.	Раздел 5. Активный аудит моделей безопасности	2		6	2	12	4	20	
6.	Раздел 6. Модель систем военных сообщений	2		6	2	12	4	20	
	Экзамен							36	
	Итого:	**12**		**28**	**8**	**68**	**20**	**144**	

2.4. Планы теоретических (лекционных) занятий

№	Наименование тем лекций	Кол-во часов в 1 семестре
1 семестр		
Раздел 1. Основные понятия теории компьютерной безопасности.		
1.	Структура теории компьютерной безопасности. Основные уровни защиты информации.	2
Раздел 2. Политики безопасности		
1.	Политики (стратегии) безопасности.	2
Раздел 3. Дискреционная политика разграничения доступа		
1.	Модели систем разграничения, распространения доступа	2
Раздел 4. Мандатная политика разграничения доступа		
1.	Классическая модель системы безопасности	2
Раздел 5. Активный аудит моделей безопасности		
1.	Общая архитектура и методы анализа систем безопасности анализа	2
Раздел 6. Модель систем военных сообщений		
1.	Неформальное и формальное описание модели систем военных сообщений	2

2.5. Планы практических (семинарских) занятий

№	Наименование практических занятий	Кол-во часов в 1 семестре
1 семестр		
Раздел 1. Основные понятия теории компьютерной безопасности.		
1.	Язык. Объекты. Субъекты. Доступ. Ценность информации.	2
2.	Аддитивная модель. Порядковая шкала. Решетка ценности.	2
Раздел 2. Политики безопасности		
1.	Политика ролевого разграничения доступа	2
2.	Политика изолированной программной среды.	2
Раздел 3. Дискреционная политика разграничения доступа		
1.	Модель Харрисона-Руззо-Ульмана.	2
2.	Модель распространения прав доступа Take-Grant.	2
Раздел 4. Мандатная политика разграничения доступа		
1.	Модель Белла-ЛаПадулы.	2
2.	Функция переходов и ее безопасность в смысле администрирования в классической модели Белла-ЛаПадула.	2
Раздел 5. Активный аудит моделей безопасности		
1.	Сигнатурный анализ. Теорема Клини	2
2.	Статистический анализ. Алгоритм NIDES	2
3.	Декомпозиция и восстановление многоуровневой базы данных	2
Раздел 6. Модель систем военных сообщений		
1.	Неформальное описание модели систем военных сообщений.	2
2.	Формальное описание модели систем военных сообщений.	2
3.	Безопасность переходов в модели систем военных сообщений.	2

2.6. Планы лабораторных работ – не предусмотрено.

2.7. Планы самостоятельной работы обучающегося по дисциплине (модулю).

№	Название разделов и тем	Виды самостоятельной работы	Трудоемкость	Формируемые компетенции	Формы контроля
1.	Раздел 1. Основные понятия теории компьютерной безопасности.	Самоподготовка по теме: Анализ угроз информационной безопасности. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы. Структура теории компьютерной безопасности. Основные уровни защиты информации. Защита машинных носителей информации и средств взаимодействия. Защита представления информации.	8	ПК-6	Устный опрос
2.	Раздел 2. Политики безопасности	Самоподготовка по теме: Дискреционная политика разграничения доступа. Мандатная (пол-номочная) политика разграничения доступа.	12	ПК-6	Устный опрос
3.	Раздел 3. Дискреционная политика разграничения доступа	Самоподготовка по теме: Модель Харрисона-Руззо-Ульмана. Модель распространения прав доступа Take-Grant. Разрешимость проблемы безопасности. Расши-ренная модель Take-Grant. Анализ информационных каналов.	12	ПК-6	Устный опрос
4.	Раздел 4. Мандатная политика разграничения доступа	Самоподготовка по теме: По-литика low-watermark в модели Белла-ЛаПадула. Условия и резуль-таты выполнения операций при реализации политики low-watermark в модели Белла-ЛаПадула. Безопасность переходов в классической модели Белла-ЛаПадула. Функция переходов и ее безопасность в смысле администрирования в классической модели Белла-ЛаПадула. Модель мандатной политики целостности информации Биба.	12	ПК-6	Устный опрос
5.	Раздел 5. Активный аудит моделей безопасности	Самоподготовка по теме:	12	ПК-6	Устный опрос
6.	Раздел 6.	Самоподготовка по теме:	12	ПК-6	Устный

	Модель систем военных сообщений	Определения смыслов безопасности функции переходов в модели систем во-енных сообщений. Базовая теорема безопасности в модели систем военных сообщений. Теорема о безопасности системы в модели систем военных сообщений.			опрос

2.8. Планы практической подготовки

Очная форма обучения

№	Наименование тем и элементов работ, связанных с будущей профессиональной деятельностью	Форма проведения (ЛПП, ПЗПП, ЛРПП, СРПП)	Кол-во часов 1 семестре
1.	**Раздел 1. Основные понятия теории компьютерной безопасности.**	ПЗПП	
		СРПП	2
2.	**Раздел 2. Политики безопасности**	ПЗПП	
		СРПП	2
3.	**Раздел 3. Дискреционная политика разграничения доступа**	ПЗПП	2
		СРПП	4
4.	**Раздел 4. Мандатная политика разграничения доступа**	ПЗПП	2
		СРПП	4
5.	**Раздел 5. Активный аудит моделей безопасности**	ПЗПП	2
		СРПП	4
6.	**Раздел 6. Модель систем военных сообщений**	ПЗПП	2
		СРПП	4
	Итого:	ПЗПП	8
		СРПП	20

3. ОСОБЕННОСТИ ОБУЧЕНИЯ ЛИЦ С ОВЗ (ПОДА)

При организации обучения студентов с инвалидностью и ОВЗ (ПОДА) обеспечиваются следующие необходимые условия:

- учебные занятия организуются исходя из психофизического развития и состояния здоровья лиц с ОВЗ совместно с другими обучающимися в общих группах, а также индивидуально, в соответствии с графиком индивидуальных занятий;

- при организации учебных занятий в общих группах используются социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений, создания комфортного психологического климата в группе;

- в процессе образовательной деятельности применяются материально-техническое оснащение, специализированные технические средства приема-передачи учебной информации в доступных формах для студентов с различными нарушениями, электронные образовательные ресурсы в адаптированных формах.

- подбор и разработка учебных материалов преподавателями производится с учетом психофизического развития и состояния здоровья лиц с ОВЗ;

- используются элементы дистанционного обучения при работе со студентами, имеющими затруднения с моторикой;

- при необходимости студенты с инвалидностью и ОВЗ обеспечиваются текстами конспектов (при затруднении с конспектированием);

- при проверке усвоения материала используются методики, не требующие выполнения рукописных работ или изложения вслух (при затруднениях с письмом и речью).

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине обеспечивается выполнение следующих дополнительных требований в зависимости от индивидуальных особенностей обучающихся:

- инструкция по порядку проведения процедуры оценивания предоставляется в доступной форме (устно, в письменной форме, на электронном носителе, в печатной форме увеличенным шрифтом и т.п.);

- доступная форма предоставления заданий оценочных средств (в печатной форме, в печатной форме увеличенным шрифтом, в форме электронного документа);

- доступная форма предоставления ответов на задания (письменно на бумаге, набор ответов на компьютере, устно, др.).

При необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная работа. Под индивидуальной работой подразумевается две формы взаимодействия с преподавателем: индивидуальная учебная работа (консультации), т.е. дополнительное разъяснение учебного материала и углубленное изучение материала с теми обучающимися, которые в этом заинтересованы, и индивидуальная воспитательная работа. Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или обучающимся с ограниченными возможностями здоровья.

4. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Самостоятельная работа студентов представляет собой обязательный вид деятельности, обеспечивающий успешное освоение образовательной программы высшего образования в соответствии с требованиями ФГОС.

Самостоятельная работа в рамках образовательного процесса решает следующие задачи:

- закрепление и расширение знаний, умений, полученных студентами во время аудиторных и внеаудиторных занятий;
- приобретение дополнительных знаний и навыков по изучаемой дисциплине;
- формирование и развитие знаний и навыков, связанных с научно-исследовательской деятельностью;
- развитие навыков самоорганизации;
- формирование самостоятельности мышления, способности к саморазвитию, самосовершенствованию и самореализации;
- выработка навыков эффективной самостоятельной профессиональной теоретической, практической и учебно-исследовательской деятельности.

Основными принципами организации самостоятельной работы являются:

- принцип обратной связи, позволяющий осуществлять контроль и коррекцию действий студента;

- принцип развития интеллектуального потенциала студента (формирование алгоритмического, наглядно-образного, теоретического стилей мышления, умений принимать оптимальные или вариативные решения в сложной ситуации, умений обрабатывать информацию);
- принцип обеспечения целостности и непрерывности обучения (предоставление возможности последовательного выполнения заданий в пределах темы, дисциплины).

Основными видами самостоятельной работы по данной дисциплине являются подготовка к практическому занятию, подготовка к контрольной работе, подготовка к тесту, подготовка к экзамену.

Подготовка к практическому занятию требует поиска дополнительной информации по теме, которой будет посвящено занятие, что позволяет глубже разобраться в изучаемых вопросах и сформировать навык самостоятельного информационного поиска и анализа подобранного материала. При подготовке к практическим занятиям студенту рекомендуется придерживаться следующего порядка:

- внимательно изучить основные вопросы темы практического занятия, определить место темы занятия в общем содержании, ее связь с другими темами;
- найти и проработать соответствующие разделы в рекомендованных учебниках, нормативных документах и дополнительной литературе;
- после ознакомления с теоретическим материалом ответить на вопросы для самопроверки;
- продумать свое понимание сложившейся ситуации в изучаемой сфере, пути и способы решения проблемных вопросов;
- продумать развернутые ответы на предложенные вопросы темы, опираясь на лекционные материалы, расширяя и дополняя их данными из учебников, дополнительной литературы.

Подготовка к контрольной работе. Контрольная работа проводиться после изучения определенной темы (тем) дисциплины и представляет собой совокупность развернутых письменных ответов студентов на вопросы, которые они получают от преподавателя. Самостоятельная подготовка к контрольной работе включает в себя:

- изучение конспектов лекций, раскрывающих материал, знание которого проверяется контрольной работой;
- повторение учебного материала, полученного при подготовке к практическим занятиям и во время их проведения;
- изучение дополнительной литературы, в которой конкретизируется содержание проверяемых знаний.

Подготовка к тестированию. Тестирование – это не только форма контроля, но и метод углубления, закрепления знаний обучающихся. Задача тестирования - добиться глубокого изучения отобранного материала, пробудить у обучающегося стремление к изучению дополнительной литературы. Подготовка включает в себя изучение рекомендованной литературы, лекционного материала, конспектирование дополнительных источников. Чтение и запоминание текста индивидуально. Желательно сначала прочитать текст целиком, потом выделить в нем главные мысли, разделить текст на части, составить план текста, выделить логическую связь между этими пунктами и потом еще раз перечитать и пересказать.

Подготовка к опросу включает в себя повторение пройденного материала по теме предстоящего опроса. Помимо основного материала студент должен изучить дополнительную рекомендованную литературу и информацию по теме, в том числе с использованием Интернет-ресурсов. Опрос предполагает устный ответ студента на один основной и несколько дополнительных вопросов преподавателя. Ответ студента должен представлять собой развёрнутое, связанное, логически выстроенное сообщение. При выставлении оценки преподаватель учитывает правильность ответа по содержанию, его

последовательность, самостоятельность суждений и выводов, умение связывать теоретические положения с практикой, в том числе и с будущей профессиональной деятельностью.

Подготовка к зачету. Подготовка к зачету осуществляется на протяжении всего периода освоения учебной дисциплины, но непосредственную подготовку в период промежуточной аттестации целесообразно осуществлять в два этапа. На первом из разных источников подбирается весь материал, необходимый для развернутых ответов на все вопросы. При ознакомлении с каким-либо разделом учебника рекомендуется прочитать его целиком, стараясь уловить логику и основную мысль автора. При вторичном чтении лучше акцентировать внимание на основных, ключевых вопросах темы. Можно составить краткий конспект, что позволит изученный материал быстро освежить в памяти перед экзаменом. Конспектирующему следует выделять понятия, категории, законы, принципы, идеи выводы, факты и т. д. Затем выявляются связи и отношения между этими компонентами текста. Технологические приемы конспектирования: выписки цитат; пересказ своими словами; выделение идей и теорий; критические замечания; уточнения; собственные разъяснения; сравнивание позиций; реконструкция текста в виде создания таблиц, рисунков, схем; описание связей и отношений; введение дополнительной информации и др. Хороший конспект отличается краткостью - не более 1/8 первичного текста, целевой направленностью, научной корректностью, ясностью, четкостью, понятностью. Важно отметить сложные и непонятные места, чтобы на консультации задать вопрос преподавателю. На втором этапе по памяти восстанавливается содержание того, что записано в ответах на каждый вопрос.

Контроль самостоятельной работы студента осуществляется посредством текущего и промежуточного контроля. Текущий контроль осуществляется на практических занятиях в ходе проверки отдельных видов самостоятельной работы, выполненной студентами. Промежуточный контроль самостоятельной работы осуществляется в ходе промежуточной аттестации обучающихся.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

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

6. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

6.1. Организация входного, текущего и промежуточного контроля обучения

Входное тестирование – не предусмотрено.
Текущий контроль – устный опрос.
Промежуточная аттестация – экзамен.

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

Не предусмотрены.

6.3. Курсовая работа

Не предусмотрено.

6.4. Вопросы к зачету

По учебному плану не предусмотрено.

6.5. Вопросы к экзамену

1. Основные понятия теории компьютерной безопасности. Язык. Объекты. Субъекты. Доступ. Информационный поток. Основная аксиома теории защиты информации.

2. Ценность информации. Модели ценности. Решетка ценности и ее свойства.

3. Общая методология построения систем защиты.

4. Принципы построения системы защиты. Каналы утечки информации.

5. Понятие политики безопасности. Субъект-объектная модель политики безопасности.

6. Дискреционная политика безопасности. Определение. Проблема безопасности при атаке вида «Троянский конь».

7. Ролевая и мандатная политика безопасности. Определения. Политика безопасности информационных потоков.

8. Реализация политики безопасности в терминах субъект-объектной модели. Базовая теорема изолированной программной среды (ИПС).

9. Базовая теорема изолированной программной среды (ИПС). Политика изолированной программной среды.

10. Модель Харрисона-Руззо-Ульмана (HRU). Анализ безопасности модели HRU. Теоремы безопасности для модели HRU.

11. Основные положения модели Take-Grant.

12. Анализ механизмов передачи прав доступа для модели Take-Grant.

13. Расширенная модель Take-Grant. Де-факто правила и определение информационных потоков.

14. Замыкание графов доступов и информационных потоков расширенной модели Take-Grant.

15. Анализ путей распространения прав доступа и информационных потоков расширенной модели Take-Grant.

16. Классическая модель Белла-ЛаПадула. Свойства безопасности для классической модели Белла-ЛаПадула.

17. Базовая теорема безопасности для классической модели Белла-ЛаПадула.

18. Политика low-watermark в модели Белла-ЛаПадула.

19. Безопасность переходов для модели Белла-ЛаПадула.

20. Базовая теорема безопасности для модели Белла-ЛаПадула с функцией переходов. Безопасность в смысле администрирования.

21. Модель невлияния в детерминированном и вероятностном случае.

22. Скрытые каналы: содержательное определение и примеры.

23. Автоматная модель и достаточные условия невидимости канала.

24. Модель скрытого канала через Proxy- сервер.

25. Общая архитектура системы и методы анализа.

26. Сигнатурный анализ. Теорема Клини.

27. Статистический анализ. Алгоритм NIDES.

28. Состоятельность оценки числа ребер случайного графа системы безопасности.

29. Модель мандатной политики целостности информации Биба.

30. Модель системы военных сообщений (СВС). Неформальное описание модели.

31. Модель системы военных сообщений (СВС). Формальное описание модели.

32. Модель системы военных сообщений (СВС). Безопасность переходов.

6.6. Контроль освоения компетенций

Вид контроля	**Контролируемые темы (разделы)**	**Компетенции, компоненты которых контролируются**
Устный опрос	*1,2,3,4,5,6*	*ПК-6*

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

7.1.Перечень основной литературы

1. Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие / Баранова Е.К., Бабаш А.В., Ларин Д.А. - Москва: ИЦ РИОР, НИЦ ИНФРА-М, 2019. - 236 с.: - Текст: электронный. - URL: https://znanium.com/catalog/product/987215
2. Внуков, А. А. Защита информации: учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/422772

7.2.Перечень дополнительной литературы

3. Разработка высоконадежных интегрированных информационных систем управления предприятием/Капулин Д.В., Царев Р.Ю., Дрозд О.В. и др. - Красноярск: СФУ, 2015. - 184 с.: ISBN 978-5-7638-3227-3 - Текст: электронный. - URL: https://znanium.com/catalog/product/549904
4. Менеджмент риска информационной безопасности: Учебное пособие / Веселов Г.Е., Абрамов Е.С., Шилов А.К. - Таганрог: Южный федеральный университет, 2016. - 107 с.: ISBN 978-5-9275-2327-5 - Текст: электронный. - URL: https://znanium.com/catalog/product/997108
5. Информационная безопасность: Учебное пособие / Ковалев Д.В., Богданова Е.А. - Ростов-на-Дону: Южный федеральный университет, 2016. - 74 с.: ISBN 978-5-9275-2364-1 - Текст: электронный. - URL: https://znanium.com/catalog/product/997105
6. Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование: учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. — Москва: Издательство Юрайт, 2019. — 220 с. — (Университеты России). — ISBN 978-5-9916-9244-1. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/437667
7. Щеглов, А. Ю. Защита информации: основы теории: учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва: Издательство Юрайт, 2019. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/433715
8. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва: Издательство Юрайт, 2019. — 312 с. — (Специалист). — ISBN 978-5-9916-9043-0. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/437163

7.3.Программное обеспечение

1. Сетевой компьютерный класс, оснащенный современной техникой

2. Офисный программный пакет (например, Microsoft Office)
3. Web-браузер Mozilla Firefox или Google Chrome
4. Экран для проектора

7.4.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

8. 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

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

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