ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ИНКЛЮЗИВНОГО ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет Прикладная математика и информатика
Кафедра Информационных технологий и прикладной математики

УТВЕРЖДАЮ

Зав. кафедрой ПМиИ
Митрофанов Е.П.
_____
подпись

«31» августа 2021г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ (МОДУЛЯ) 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

Составитель / составители: МГГЭУ, доцент кафедры ИТиПМ
место работы, занимаемая должность


подпись

Белоглазов А.А. «21» августа 2021 г.
Ф.И.О. Дата

Рецензент: МГГЭУ, профессор кафедры ИТиПМ
место работы, занимаемая должность


подпись

Истомина Т.В. «20 » августа 2021 г .
Ф.И.О. Дата

Согласовано:

Представитель работодателя или объединения работодателей

научный сотрудника, ФГБУ ГНЦ Федеральный медицинский биофизический центр имени А.И. Бурназяна ФМБА России
(должность, место работы),


подпись

Васильев Е.В. «26 » августа 2021
Ф.И.О. Дата

Фонд оценочных средств рассмотрен и одобрен на заседании кафедры Информационных технологий и прикладной математики (протокол № 1 от «26» августа 2021 г.)

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

Дополнения и изменения, внесенные в фонд оценочных средств, утверждены на заседании кафедры _____,

протокол № _____ от «_____» _____ 20__ г.

Заведующий кафедрой _____ /

Ф.И.О/

Дополнения и изменения, внесенные в фонд оценочных средств, утверждены на заседании кафедры _____,

протокол № _____ от «_____» _____ 20__ г.

Заведующий кафедрой _____ /

Ф.И.О/

Дополнения и изменения, внесенные в фонд оценочных средств, утверждены на заседании кафедры _____,

протокол № _____ от «_____» _____ 20__ г.

Заведующий кафедрой _____ /

Ф.И.О/

Содержание

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Теоретические основы компьютерной безопасности»

Оценочные средства составляются в соответствии с рабочей программой дисциплины и представляют собой совокупность контрольно-измерительных материалов (типовые задачи (задания), контрольные работы, тесты и др.), предназначенных для измерения уровня достижения обучающимися установленных результатов обучения.

Оценочные средства используются при проведении текущего контроля успеваемости и промежуточной аттестации.

Таблица 1 - Перечень компетенций, формируемых в процессе освоения дисциплины

Код 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.

Конечными результатами освоения дисциплины являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», расписанные по отдельным компетенциям. Формирование дескрипторов происходит в течение всего семестра по этапам в рамках контактной работы, включающей различные виды занятий и самостоятельной работы, с применением различных форм и методов обучения (табл.2).

Таблица 2 - Формирование компетенций в процессе изучения дисциплины:

Код компетенции	Уровень освоения компетенций	Индикаторы достижения компетенций	Вид учебных занятий[1], работы, формы и методы обучения, способствующие формированию и развитию компетенций[2]	Контролируемые разделы и темы дисциплины[3]	Оценочные средства, используемые для оценки уровня сформированности компетенции[4]
ПК-6	Недостаточный уровень	ПК-6.1 Студент не способен самостоятельно выделять главные положения в изученном материале дисциплины. Не знает особенности современных информационных систем как объекта защиты; уязвимости основных структурно-функциональных элементов компьютерных систем; классификацию угроз безопасности; классификацию каналов проникновения в информационную систему и утечки информации; неформальную модель нарушителя; основные меры противодействия угрозам безопасности, принципы построения систем защиты, основные механизмы защиты; модели разграничения доступа;	Лекционные и практические занятия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета	Раздел 1. Основные понятия теории компьютерной безопасности. Раздел 2. Политики безопасности Раздел 3. Дискреционная политика разграничения доступа Раздел 4. Мандатная политика разграничения доступа Раздел 5. Активный аудит моделей безопасности Раздел 6. Модель систем военных сообщений	Текущий контроль – устный опрос, тестирование.

[1] Лекционные занятия, практические занятия, лабораторные занятия, самостоятельная работа…

[2] Необходимо указать активные и интерактивные методы обучения (например, интерактивная лекция, работа в малых группах, методы мозгового штурма и т.д.), способствующие развитию у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств.

[3] Наименование темы (раздела) берется из рабочей программы дисциплины.

[4] Оценочное средство должно выбираться с учетом запланированных результатов освоения дисциплины, например:
«Знать» – собеседование, коллоквиум, тест…
«Уметь», «Владеть» – индивидуальный или групповой проект, кейс-задача, деловая (ролевая) игра, портфолио…

		криптографические методы защиты			
	Базовый уровень	ПК-6.1.Студент усвоил основное содержание материала дисциплины, но имеет пробелы в усвоении материала. Имеет несистематизированные знания о особенности современных информационных систем как объекта защиты; уязвимости основных структурно-функциональных элементов компьютерных систем; классификацию угроз безопасности; классификацию каналов проникновения в информационную систему и утечки информации; неформальную модель нарушителя; основные меры противодействия угрозам безопасности, принципы построения систем защиты, основные механизмы защиты; модели разграничения доступа; криптографические методы защиты	Лекционные и практические занятия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета	Раздел 1. Основные понятия теории компьютерной безопасности. Раздел 2. Политики безопасности Раздел 3. Дискреционная политика разграничения доступа Раздел 4. Мандатная политика разграничения доступа Раздел 5. Активный аудит моделей безопасности Раздел 6. Модель систем военных сообщений	Текущий контроль – устный опрос, тестирование.

	Средний уровень	ПК-6.1. Студент способен самостоятельно выделять главные положения в изученном материале. Знает основные особенности современных информационных систем как объекта защиты; уязвимости основных структурно-функциональных элементов компьютерных систем; классификацию угроз безопасности; классификацию каналов проникновения в информационную систему и утечки информации; неформальную модель нарушителя; основные меры противодействия угрозам безопасности, принципы построения систем защиты, основные механизмы защиты; модели разграничения доступа; криптографические методы защиты	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета	Раздел 1. Основные понятия теории компьютерной безопасности. Раздел 2. Политики безопасности Раздел 3. Дискреционная политика разграничения доступа Раздел 4. Мандатная политика разграничения доступа Раздел 5. Активный аудит моделей безопасности Раздел 6. Модель систем военных сообщений	Текущий контроль – устный опрос, тестирование.

	Высокий уровень	ПК-6.1. Студент знает, понимает, выделяет главные положения в изученном материале и способен дать краткую характеристику основным идеям проработанного материала дисциплины. Знает особенности современных информационных систем как объекта защиты; уязвимости основных структурно-функциональных элементов компьютерных систем; классификацию угроз безопасности; классификацию каналов проникновения в информационную систему и утечки информации; неформальную модель нарушителя; основные меры противодействия угрозам безопасности, принципы построения систем защиты, основные механизмы защиты; модели разграничения доступа; криптографические методы защиты	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета	Раздел 1. Основные понятия теории компьютерной безопасности. Раздел 2. Политики безопасности Раздел 3. Дискреционная политика разграничения доступа Раздел 4. Мандатная политика разграничения доступа Раздел 5. Активный аудит моделей безопасности Раздел 6. Модель систем военных сообщений	Текущий контроль – устный опрос, тестирование.
	Умеет				
	Базовый уровень	Студент испытывает затруднения при осуществлении выбора 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.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета	Раздел 1. Основные понятия теории компьютерной безопасности. Раздел 2. Политики безопасности Раздел 3. Дискреционная политика разграничения доступа Раздел 4. Мандатная политика разграничения доступа Раздел 5. Активный аудит моделей безопасности Раздел 6. Модель систем	Текущий контроль – устный опрос, тестирование.

				военных сообщений	
	Средний уровень	Студент умеет на базовом уровне, 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.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета	Раздел 1. Основные понятия теории компьютерной безопасности. Раздел 2. Политики безопасности Раздел 3. Дискреционная политика разграничения доступа Раздел 4. Мандатная политика разграничения доступа Раздел 5. Активный аудит моделей безопасности Раздел 6. Модель систем военных сообщений	Текущий контроль – устный опрос, тестирование.
	Высокий уровень	Студент системно 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.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета	Раздел 1. Основные понятия теории компьютерной безопасности. Раздел 2. Политики безопасности Раздел 3. Дискреционная политика разграничения доступа Раздел 4. Мандатная политика разграничения доступа Раздел 5. Активный аудит моделей безопасности Раздел 6. Модель систем военных сообщений	Текущий контроль – устный опрос, тестирование.
	Владеет				
	Базовый уровень	Студент владеет базовыми навыками применения типовых подходов, применяемых при анализе, планировании и оперативном управлении деятельностью промышленного предприятия.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и	Раздел 1. Основные понятия теории компьютерной безопасности. Раздел 2. Политики безопасности Раздел 3. Дискреционная	Текущий контроль – устный опрос, тестирование.

			сдача промежуточной аттестации, подготовка и сдача зачета	политика разграничения доступа Раздел 4. Мандатная политика разграничения доступа Раздел 5. Активный аудит моделей безопасности Раздел 6. Модель систем военных сообщений	
	Средний уровень	Студент владеет, на среднем уровне, основными навыками применения типовых подходов, применяемых при анализе, планировании и оперативном управлении деятельностью промышленного предприятия.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета	Раздел 1. Основные понятия теории компьютерной безопасности. Раздел 2. Политики безопасности Раздел 3. Дискреционная политика разграничения доступа Раздел 4. Мандатная политика разграничения доступа Раздел 5. Активный аудит моделей безопасности Раздел 6. Модель систем военных сообщений	Текущий контроль – устный опрос, тестирование.
	Высокий уровень	Студент, на высоком уровне, владеет навыками применения типовых подходов, применяемых при анализе, планировании и оперативном управлении деятельностью промышленного предприятия.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета	Раздел 1. Основные понятия теории компьютерной безопасности. Раздел 2. Политики безопасности Раздел 3. Дискреционная политика разграничения доступа Раздел 4. Мандатная политика разграничения доступа Раздел 5. Активный аудит моделей безопасности Раздел 6. Модель систем военных сообщений	Текущий контроль – устный опрос, тестирование.

2. ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ[5]

Таблица 3

№	Наименование оценочного средства	Характеристика оценочного средства	Представление оценочного средства в ФОС
1	Устный опрос	Средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования преподавателя с обучающимися.	Вопросы по темам/разделам дисциплины
2	Тест	Средство, позволяющее оценить уровень знаний обучающегося путем выбора им одного из нескольких вариантов ответов на поставленный вопрос. Возможно использование тестовых вопросов, предусматривающих ввод обучающимся короткого и однозначного ответа на поставленный вопрос.	Тестовые задания
3	Экзамен	Средство контроля усвоения учебного материала разделов дисциплины	Вопросы к экзамену

[5] Указываются оценочные средства, применяемые в ходе реализации рабочей программы данной дисциплины.

3. ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ

Оценивание результатов обучения по дисциплине «Алгоритмизация и программирование» осуществляется в соответствии с Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся.

Предусмотрены следующие виды контроля: текущий контроль (осуществление контроля всех видов аудиторной и внеаудиторной деятельности обучающегося с целью получения первичной информации о ходе усвоения отдельных элементов содержания дисциплины) и промежуточная аттестация (оценивается уровень и качество подготовки по дисциплине в целом).

Показатели и критерии оценивания компетенций, формируемых в процессе освоения данной дисциплины, описаны в табл. 4.

Таблица 4.

Код компетенции	Уровень освоения компетенции	Индикаторы достижения компетенции	Критерии оценивания результатов обучения
ПК-6		Знает	
	Недостаточный уровень Оценка «незачтено», «неудовлетворительно»	ПК-6.*1.*	*Не знает значительной части материала курса, не способен самостоятельно выделять главные положения в изученном материале дисциплины*
	Базовый уровень Оценка, «зачтено», «удовлетворительно»	ПК-6.*1.*	*Знает не менее 50 % основного материала курса, однако испытывает затруднения в его применении*
	Средний уровень Оценка «зачтено», «хорошо»	ПК-6.*1.*	*Знает основную часть материала курса, способен применить изученный материал на практике, испытывает незначительные затруднения в решении задач*
	Высокий уровень Оценка «зачтено», «отлично»	ПК-6.*1.*	*Показывает глубокое знание и понимание материала, способен применить изученный материал на практике*
		Умеет	
	Базовый уровень	ПК-6.*2.*	*Умеет воспроизвести не менее 50 % основного материала курса, однако испытывает затруднения при решении практических задач*
	Средний уровень	ПК-6.*2.*	*Умеет решать стандартные профессиональные задачи с применением полученных знаний, испытывает незначительные затруднения в решении задач*
	Высокий уровень	ПК-6.*2.*	*Умеет решать стандартные профессиональные задачи с применением полученных знаний, показывает глубокое знание и понимание материала, способен решить задачу при изменении формулировки*
		Владеет	
	Базовый уровень	ПК-6.*3.*	*Владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности, усвоил основное содержание материала дисциплины, но имеет пробелы в усвоении материала. Имеет несистематизированные знания основных разделов дисциплины.*
	Средний уровень	ПК-6.*3.*	*Владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности, способен самостоятельно выделять главные положения в изученном материале. Испытывает незначительные затруднения в решении задач.*
	Высокий уровень	ПК-6.*3.*	*Свободно владеет навыками теоретического и экспериментального исследования, показывает глубокое знание и понимание изученного материала*

4.Методические материалы, определяющие процедуры оценивания результатов обучения

Задания в форме устного опроса:

Устный опрос используется для текущего контроля успеваемости обучающихся по дисциплине в качестве проверки результатов освоения терминологии. Каждому студенту выдается свой собственный, узко сформулированный вопрос. Ответ должен быть четким и кратким, содержащим все основные характеристики описываемого понятия, института, категории.

Задания в форме тестирования

Тест представляет собой контрольное мероприятие по учебному материалу каждой темы (раздела) дисциплины, состоящее в выполнении обучающимся системы стандартизированных заданий, которая позволяет автоматизировать процедуру измерения уровня знаний и умений обучающегося.

Тестирование является средством текущего контроля успеваемости обучающихся по дисциплине и может включать в себя следующие типы заданий: задание с единственным выбором ответа из предложенных вариантов, задание на определение верных и неверных суждений; задание с множественным выбором ответов.

В каждом задании необходимо выбрать все правильные ответы.

5. Материалы для проведения текущего контроля и промежуточной аттестации

Задания в форме устного опроса

Перечень вопросов модульного блока №1

1. Введите определение:

□□*аддитивная модель*
□□*анализ риска*
□□безопасность данных
□□безопасность информации
□□*доступ*
□□доступность
□□защита информации
□□защищенность
□□*злоумышленник*
□□*злоумышленные бедствия*
□□*идентификация угроз*
□□информационная безопасность
□□*каталоги (таксономические схемы классификации) угроз безопасности*

классификация угроз

□□конфиденциальность
□□*нарушитель*
□□*несанкционированный доступ к данным*
□□носитель угрозы
□□общая модель процесса нарушения защищенности информации
□□*объект доступа*
□□объекты безопасности
□□*опишите популярные методы проведения анализа риска*
□□основные этапы развития теории и практики КБ
□□*особенности информационных ресурсов*:
□□*отказ*

□□*ошибка*
□□*перечислите общие принципы обеспечения КБ*
□□*побочные явления*
□□*порядковая шкала ценностей*
□□последствия угрозы
□□*представьте парно-субъектную модель конкурирующего взаимодействия*
□□*ресурс*
□□*сбой*
□□секретность
□□*стихийные бедствия*
□□структура *защищаемой информации*
□□*субъект доступа*
□□сущность угрозы
□□угрозы безопасности информации
□□*факторы, воздействующие на информацию*
□□*физическая целостность*
□□целостность
□□*целостность данных*
□□*ценность информации*

2. Опишите основные исследования российских научных школ в сфере ИБ
3. Опишите сущность принципа комплексности
4. Опишите сущность принципа разумной достаточности
5. Опишите сущность принципа системности
6. Опишите сущность принципа целенаправленности
7. Перечислите типы ДСФ
8. Опишите типы информации, используемой для принятия решения в задаче поведения
9. Опишите типы классификаций
10. Перечислите требования к информации с точки зрения её безопасности (доступа к ней)
11. Перечислите угрозы по направлению осуществления
12. Перечислите угрозы по природе происхождения
13. Перечислите уровни информационной безопасности

Перечень вопросов модульного блока №2

1. Введите определение: Идентификация. Аутентификация НСД.
2. Структура дерева угроз
3. Идентификация угроз
4. Структура потенциальных нарушителей (злоумышленников)
5. Опишите базовые составляющие ИБ
6. Как оцениваются риски
7. Модель нарушителя
8. Модель системы защиты с полным перекрытием
9. Модель внутреннего нарушителя по РД ГосТехКомисии
10. Как рассчитываются ожидаемые одноразовые потери
11. Как рассчитываются ежегодные потери
12. Опишите сущность методов оценивания вероятности угроз
13. Перечислите методики экспертных оценок
14. Перечислите принципы защиты информации
15. Перечислите цели защиты информации
16. Перечислите основные задачи системы защиты информации

17. Опишите средства защиты информации
18. Перечислите требования к системам защиты информации
19. Перечислите методы и технологии обеспечения конфиденциальности данных
20. Перечислите методы и технологии обеспечения целостности данных
21. Перечислите методы и технологии обеспечения доступности данных
22. Перечислите основные компоненты парольной системы
23. Организационно-режимные меры защиты носителей информации в компьютерных системах
24. Опишите основные задачи обеспечения информационной безопасности ИС от угрозы раскрытия конфиденциальности на уровне МНИ
25. Опишите парольные системы для защиты от несанкционированного доступа к ин-формации
26. Опишите группы методов аутентификации
27. Опишите общие подходы к построению парольных систем
28. Передача пароля по сети
29. Опишите средства криптографической защиты информации
30. Опишите классификационную структуру каналов утечки информации
31. Опишите требования к средствам криптографической защиты информации

Опишите способы и особенности реализации криптографических подсистем
33. Перечислите принципы, обеспечивающие целостность данных в ИС
34. Перечислите формы атак на объекты информационных систем
35. Опишите модель контроля целостности данных на примере модели Кларка-Вильсона
36. Опишите особенности обеспечения целостности информации барьерных адресов
37. Опишите особенности обеспечения целостности информации в динамических областях памяти
38. Опишите особенности обеспечения целостности информации в адресных регистрах
39. В чем заключается сущность защиты от сбоев программно-аппаратной среды
40. Как обеспечить отказоустойчивость программного обеспечения компьютерной системы
41. Как предотвратить неисправности в программном обеспечении компьютерных систем
42. Как реализуется защита семантического анализа и актуальности информации

Перечень вопросов модульного блока №3

1. Структура СЗИ
2. Политика безопасности организации
3. Политика безопасности КС
4. Процесс разработки политики безопасности
5. Неформальное описания политики безопасности
6. Модель безопасности
7. Субъектно-объектные модели КС
8. Аксиомы защищенности компьютерных систем
9. Монитор безопасности: определение (МБ, МБО, МБС), требования
10. Объекты (Субъекты) тождественные, порожденные, корректные, абсолютно корректные, изолированные,
11. Изолированная программная среда
12. Базовая теорема ИПС

13. Общая характеристика политики дискреционного доступа
14. Виды политик (правил, механизмов) разграничения доступа
15. Общая характеристика моделей полномочного (мандатного) доступа
16. Общая характеристика тематического разграничения доступа
17. Пятимерное пространство Хартсона
18. Модели на основе матрицы доступа
19. Модели распространения прав доступа
20. Модель Харрисона-Руззо-Ульмана (модель HRU)
21. Модель типизованной матрицы доступа (модель TAM)
22. Теоретико-графовая модель TAKE-GRANT
23. Достоинства и недостатки дискреционных моделей
24. Модель Белла-ЛаПадулы
25. Достоинства и недостатки модели Белла-ЛаПадулы
26. Расширения модели Белла-ЛаПадулы
27. Модель тематико-иерархического разграничения доступа
28. Модели ролевого доступа
29. Разновидности организации ролей
30. Модели индивидуально-группового доступа
31. MMS (militarymessagesystem)-модель
32. Ограничения безопасности в MMS-модели

Контролируемые компетенции: ПК-6.
Оценка компетенций осуществляется в соответствии с таблицей 4.

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.

Контролируемые компетенции: ПК-6.
Оценка компетенций осуществляется в соответствии с таблицей 4.