ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ИНКЛЮЗИВНОГО ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»

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»
Зав. кафедрой _____
«26» августа 2019

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

«Современные методы и средства защиты информации»

Образовательная программа направления подготовки

01.04.02 Прикладная математика и информатика

Блок Б1.О.10 «Дисциплины (модули)», обязательная часть

Профиль подготовки

Математическое и программное обеспечение информационных систем в прикладных областях

Квалификация (степень) выпускника

Магистр

Форма обучения очная

Курс 1, семестр 2

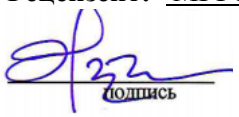
Москва

2019

Составители рабочей программы: МГГЭУ, доцент кафедры ИМиПМ
место работы, занимаемая должность


подпись Петрунина Е.В. «20» августа 2019 г.
Ф.И.О. Дата

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



Никольский А.Е. «21» августа 2019 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 2019 г.
Ф.И.О. Дата

Фонд оценочных средств рассмотрен и одобрен на заседании кафедры Информационных технологий и прикладной математики (протокол № 1 от «26» августа 2019 г.)

/Зав. кафедрой ИТиПМ/  Петрунина Е.В. «26» августа 2019 г.
подпись 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 «Современные методы и средства защиты информации»

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	**Наименование результата обучения**
ОПК-4	Способен комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности
	ОПК-4.1 Знает основные методы получения новых знаний с помощью информационных технологий для решения задач в области профессиональной деятельности с учетом требований информационной безопасности; стандарты оформления программной документации и причины нарушения компьютерной безопасности. ОПК-4.2 Умеет применять информационные технологии в практической деятельности и анализировать полученные решения вычислительных задач; на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств защиты информации; ориентироваться в современных и перспективных математических методах защиты информации. ОПК-4.3 Владеет информационными технологиями как средством получения новых знаний; методами информационной и кадровой безопасности в коммуникационной деятельности.

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]
ОПК-4		*Знает*			
	Недостаточный уровень	ОПК-4. Студент не способен самостоятельно выделять главные положения в изученном материале дисциплины. Не знает основные методы получения новых знаний с помощью информационных технологий для решения задач в области профессиональной деятельности с учетом требований информационной безопасности; стандарты оформления программной документации и причины	Лекционные и практические занятия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача экзамена.	1. Введение 2. Защита информации от ПЭМИН 3. Основы теории защиты информации в компьютерных системах 4. Основы криптографии 5. Применение симметричных криптосистем для защиты компьютерной информации 6. Инфраструктура открытых ключей 7. Методы идентификации и аутентификации пользователей компьютерных систем 8. Защита компьютерных систем от	Текущий контроль – устный опрос.

[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…

		нарушения компьютерной безопасности.		удаленных атак через сеть Internet 9. Методы защита программ от изучения и разрушающих программных воздействий (программных закладок и вирусов)	
	Базовый уровень	ОПК-4.1. Студент усвоил основное содержание материала дисциплины, но имеет пробелы в усвоении материала. Имеет несистематизированные знания об основных методах получения новых знаний с помощью информационных технологий для решения задач в области профессиональной деятельности.	Лекционные и практические занятия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача экзамена.	1. Введение 2. Защита информации от ПЭМИН 3. Основы теории защиты информации в компьютерных системах 4. Основы криптографии 5. Применение симметричных криптосистем для защиты компьютерной информации 6. Инфраструктура открытых ключей 7. Методы идентификации и аутентификации пользователей компьютерных систем 8. Защита компьютерных систем от удаленных атак через сеть Internet 9. Методы защита программ от изучения и разрушающих программных воздействий (программных закладок и вирусов)	Текущий контроль – устный опрос.
	Средний уровень	ОПК-4.1. Студент способен самостоятельно выделять главные положения в изученном материале. Знает основные методы получения новых знаний с помощью информационных технологий для решения задач в области профессиональной деятельности с учетом	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача экзамена.	1. Введение 2. Защита информации от ПЭМИН 3. Основы теории защиты информации в компьютерных системах 4. Основы криптографии 5. Применение симметричных криптосистем для защиты компьютерной информации 6. Инфраструктура открытых ключей	Текущий контроль – устный опрос.

		требований информационной безопасности.		7. Методы идентификации и аутентификации пользователей компьютерных систем 8. Защита компьютерных систем от удаленных атак через сеть Internet 9. Методы защита программ от изучения и разрушающих программных воздействий (программных закладок и вирусов)	
	Высокий уровень	ОПК-4.1. Студент знает, понимает, выделяет главные положения в изученном материале и способен дать краткую характеристику основным идеям проработанного материала дисциплины. Показывает глубокое знание и понимание основных методов получения новых знаний с помощью информационных технологий для решения задач в области профессиональной деятельности с учетом требований информационной безопасности; стандартов оформления программной документации и причин нарушения компьютерной безопасности.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача экзамена.	1. Введение 2. Защита информации от ПЭМИН 3. Основы теории защиты информации в компьютерных системах 4. Основы криптографии 5. Применение симметричных криптосистем для защиты компьютерной информации 6. Инфраструктура открытых ключей 7. Методы идентификации и аутентификации пользователей компьютерных систем 8. Защита компьютерных систем от удаленных атак через сеть Internet 9. Методы защита программ от изучения и разрушающих программных воздействий (программных закладок и вирусов)	Текущий контроль – устный опрос.
		Умеет			

	Базовый уровень	ОПК-4.2. Студент испытывает затруднения при применении информационных технологий в практической деятельности. Студент непоследовательно анализирует полученные решения вычислительных задач.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача экзамена.	1. Введение 2. Защита информации от ПЭМИН 3. Основы теории защиты информации в компьютерных системах 4. Основы криптографии 5. Применение симметричных криптосистем для защиты компьютерной информации 6. Инфраструктура открытых ключей 7. Методы идентификации и аутентификации пользователей компьютерных систем 8. Защита компьютерных систем от удаленных атак через сеть Internet 9. Методы защита программ от изучения и разрушающих программных воздействий (программных закладок и вирусов)	Текущий контроль – устный опрос.
	Средний уровень	ОПК-4.2. Студент умеет применять информационные технологии в практической деятельности и анализировать полученные решения вычислительных задач; на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств защиты информации.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача экзамена.	1. Введение 2. Защита информации от ПЭМИН 3. Основы теории защиты информации в компьютерных системах 4. Основы криптографии 5. Применение симметричных криптосистем для защиты компьютерной информации 6. Инфраструктура открытых ключей 7. Методы идентификации и аутентификации пользователей компьютерных систем	Текущий контроль – устный опрос.

				8. Защита компьютерных систем от удаленных атак через сеть Internet 9. Методы защита программ от изучения и разрушающих программных воздействий (программных закладок и вирусов)	
	Высокий уровень	ОПК-4.2. Студент умеет самостоятельно применять информационные технологии в практической деятельности и анализировать полученные решения вычислительных задач; на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств защиты информации; ориентироваться в современных и перспективных математических методах защиты информации.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача экзамена.	1. Введение 2. Защита информации от ПЭМИН 3. Основы теории защиты информации в компьютерных системах 4. Основы криптографии 5. Применение симметричных криптосистем для защиты компьютерной информации 6. Инфраструктура открытых ключей 7. Методы идентификации и аутентификации пользователей компьютерных систем 8. Защита компьютерных систем от удаленных атак через сеть Internet 9. Методы защита программ от изучения и разрушающих программных воздействий (программных закладок и вирусов)	Текущий контроль – устный опрос.
		Владеет			

	Базовый уровень	ОПК-4.3. Студент владеет основными информационными технологиями как средством получения новых знаний.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача экзамена.	1. Введение 2. Защита информации от ПЭМИН 3. Основы теории защиты информации в компьютерных системах 4. Основы криптографии 5. Применение симметричных криптосистем для защиты компьютерной информации 6. Инфраструктура открытых ключей 7. Методы идентификации и аутентификации пользователей компьютерных систем 8. Защита компьютерных систем от удаленных атак через сеть Internet 9. Методы защита программ от изучения и разрушающих программных воздействий (программных закладок и вирусов)	Текущий контроль – устный опрос.

	Средний уровень	ОПК-4.3. Студент владеет информационными технологиями как средством получения новых знаний; методами информационной безопасности.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача экзамена.	1. Введение 2. Защита информации от ПЭМИН 3. Основы теории защиты информации в компьютерных системах 4. Основы криптографии 5. Применение симметричных криптосистем для защиты компьютерной информации 6. Инфраструктура открытых ключей 7. Методы идентификации и аутентификации пользователей компьютерных систем 8. Защита компьютерных систем от удаленных атак через сеть Internet 9. Методы защита программ от изучения и разрушающих программных воздействий (программных закладок и вирусов)	Текущий контроль – устный опрос.
	Высокий уровень	ОПК-4.3. Студент владеет знаниями всего изученного материала, владеет информационными технологиями как средством получения новых знаний; методами информационной и кадровой безопасности в коммуникационной деятельности.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача экзамена.	1. Введение 2. Защита информации от ПЭМИН 3. Основы теории защиты информации в компьютерных системах 4. Основы криптографии 5. Применение симметричных криптосистем для защиты компьютерной информации 6. Инфраструктура открытых ключей 7. Методы идентификации и	Текущий контроль – устный опрос.

				аутентификации пользователей компьютерных систем 8. Защита компьютерных систем от удаленных атак через сеть Internet 9. Методы защита программ от изучения и разрушающих программных воздействий (программных закладок и вирусов)	

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

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

3. ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ

Оценивание результатов обучения по дисциплине «Современные методы и средства защиты информации» 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
ОПК-4		Знает	
	Недостаточный уровень Оценка «неудовлетворительно»	*ОПК-4.1.*	*Не знает значительной части материала курса, не способен самостоятельно выделять главные положения в изученном материале дисциплины*
	Базовый уровень Оценка «удовлетворительно»	*ОПК-4.1.*	*Знает не менее 50 % основного материала курса, однако испытывает затруднения в его применении*
	Средний уровень Оценка «хорошо»	*ОПК-4.1.*	*Знает основную часть материала курса, способен применить изученный материал на практике, испытывает незначительные затруднения в решении задач*
	Высокий уровень Оценка «отлично»	*ОПК-4.1.*	*Показывает глубокое знание и понимание материала, способен применить изученный материал на практике*
		Умеет	
	Базовый уровень	*ОПК-4.2.*	*Умеет воспроизвести не менее 50 % основного материала курса, однако испытывает затруднения при решении практических задач*
	Средний уровень	*ОПК-4.2.*	*Умеет решать стандартные профессиональные задачи с применением полученных знаний, испытывает незначительные затруднения в решении задач*
	Высокий уровень	*ОПК-4.2.*	*Умеет решать стандартные профессиональные задачи с применением полученных знаний, показывает глубокое знание и понимание материала, способен решить задачу при изменении формулировки*
		Владеет	
	Базовый уровень	*ОПК-4.3.*	*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	*ОПК-4.3.*	*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	*ОПК-4.3.*	*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.

5. Материалы для проведения текущего контроля и промежуточной аттестации

Задания в форме устного опроса

Семестр 2

1. Организационно-правовые вопросы защиты информации
2. Каналы утечки информации из компьютерных систем
3. Пассивные и активные методы защиты
4. Критерии информационной безопасности.
5. Основные понятия теории защиты информации
6. Угрозы безопасности
7. Математические модели политики безопасности
8. Общие критерии безопасности информационных технологий
9. Понятия и определения; классификация шифров
10. Блочные и поточные шифры
11. Поля Фейстеля
12. Стандарт шифрования данных DES
13. Отечественный стандарт шифрования данных
14. Концепция криптосистемы с открытым ключом
15. Однонаправленные функции
16. Криптосистемы шифрования данных RSA и Эль Гамаля
17. Аутентификация данных
18. Алгоритмы безопасного хеширования
19. ЭЦП криптосистем RSA и Эль Гамаля
20. Алгоритм цифровой подписи DSA
21. Отечественные алгоритмы цифровой надписи
22. Применение межсетевых экранов для организации виртуальных корпоративных сетей
23. Системы организации защищенного документооборота
24. Криптопротоколы.
25. Методы внедрения программных закладок; компьютерные вирусы и антивирусные программы
26. Классификация вирусов
27. Защита от разрушающих программных воздействий
28. Проблемы компьютерной безопасности
29. Перспективные направления исследований

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

Темы курсовых работ

Не предусмотрено

Вопросы к зачету

Не предусмотрено

Вопросы к экзамену

Семестр 2

1. Современные аспекты безопасности информационных систем.
2. Понятие «информационная безопасность» и «защита информации».
3. Назначение организационных средств защиты
4. Состав комплекса защиты территории охраняемых объектов
5. Понятие информационного права.
6. Степени секретности и виды конфиденциальности информации.
7. Понятие информации, изъятой из оборота, и ограниченной в обороте.
8. Нормативные документы по лицензированию деятельности
9. Нормативные документы по сертификации средств защиты
10. Понятие ПЭМИН
12. Методы защиты компьютеров от утечки ПЭМИН.
13. Назначение генератора шума.
14. Классификация угроз безопасности.
15. Назначение средств защиты от НДС.
16. Основные свойства защищаемой информации.
17. Понятие политики безопасности
18. Состав системы разграничения доступа
19. Матричная модель системы ЗИ.
20. Многоуровневая модель системы ЗИ.
21. Система регистрации
22. Критерии оценки безопасности компьютерных систем министерства обороны США(«Оранжевая книга»)
23. Руководящий документ (РД) Гостехкомиссии России «Классификация автоматизированных систем и требования по ЗИ»
24. Сравнительный анализ «Оранжевой книги» и РД
25. Криптографическая защита информации в каналах связи и компьютерах.
26. Основные термины и понятия криптографии.
27. Классификация криптосистем.
28. Симметричные криптосистемы. Классификация шифров
29. Блочные и поточные шифры

30. Требования к криптосистемам.
31. Гаммирование.
32. Аппаратные и программные генераторы псевдослучайных чисел (ПСЧ)
33. Составные шифры
34. Криптосистема «ЛЮЦИФЕР».
35. Поля Фейстеля
36. Алгоритм криптосистемы DES.
37. Режимы шифрования криптосистемы DES.
38. Отечественный алгоритм шифрования ГОСТ 28147-89
39. Режимы шифрования криптосистемы ГОСТ 28147-89
40. Сравнительный анализ криптосистем DES и ГОСТ 28147-89.
41. Концепция криптосистемы с открытым ключом.
42. Однонаправленные функции.
43. Классификация алгоритмов двухключевых систем.
44. Алгоритмы рюкзака.
45. Алгоритм RSA.
46. Схема шифрования Эль-Гамаля.
47. ЭЦП Эль-Гамаля.
48. Генерация и рассылка ключей.
49. Хранение и уничтожение ключей.
50. Понятия идентификации, аутентификации и авторизации.
51. Парольная аутентификация.
52. Взаимная проверка пользователей.
53. Система Kerberos.
54. Аутентификация удаленных пользователей.
55. Назначение однонаправленных хэш-функций.
56. Алгоритм безопасного хеширования SHA.
57. Отечественный стандарт хэш-функции.
58. Алгоритм цифровой подписи RSA.
59. Алгоритм цифровой подписи Эль Гамаля (EGSA).
60. Алгоритм цифровой подписи DSA.
61. Отечественные алгоритмы ЭЦП.
62. Понятие атаки на компьютерную систему.
63. Типичные угрозы в среде Internet.
64. Программно-аппаратные методы защиты от удаленных атак в сети Internet.
65. Методика Firewall, реализуемая на базе программно-аппаратных средств.
66. Назначение Proxy-сервера.
67. Сетевой монитор безопасности.
68. Назначение СОВ.
69. Туннелирование на канальном уровне. Протоколы PPTP и L2TP.
70. Туннелирование на сетевом уровне. Архитектура IPSec.
71. Защита соединения на сеансовом уровне. Протоколы SSL и TLS.
72. Классификация способов защиты от от изучения и разрушающих программных воздействий.

73. Методы перехвата и навязывания информации.
74. Методы внедрения программных закладок.
75. История возникновения компьютерных вирусов.
76. Классификация вирусов.
77. Детекторы, фаги, прививки.
78. Вакцины, ревизоры и мониторы.
79. Проблемы компьютерной безопасности.
80. Перспективные направления исследований в компьютерной безопасности.