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

Факультет Прикладная математика и информатика
Кафедра Цифровых технологий

УТВЕРЖДАЮ
Проректор по учебно-методической работе
_____ Сахарчук Е.С.
«27» 01 2022 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ (МОДУЛЯ) СОВРЕМЕННЫЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

образовательная программа направления подготовки
01.04.02 "Прикладная математика и информатика"
Б1.О.09 «Дисциплины (модули)», обязательная часть

Профиль подготовки
Математическое и информационное обеспечение цифровой экономики

Квалификация (степень) выпускника
Магистр

Форма обучения: очная

Курс 1 семестр 2

Москва
2022

Разработчики (и): МГГЭУ, заведующий кафедрой цифровых технологий
место работы, занимаемая должность

_____ Митрофанов Е.П. 14.03 2022 г
подпись Ф.И.О. Дата

Фонд оценочных средств рассмотрен и одобрен на заседании кафедры
цифровых технологий
(протокол № 4 от « 21 » 03 2022 г.)

на заседании Учебно-методического совета МГГЭУ
(протокол № 1 от « 27 » 04 2022 г.)

Согласовано:

Представитель работодателя
или объединения работодателей _____ / Демидов Л.Н. /
АО «Микропроцессорные системы»
к.т.н., доцент
(должность, место работы)
« 21 » 03 2022 г.

СОГЛАСОВАНО:

Начальник учебно-методического управления
_____ И.Г. Дмитриева
« 27 » 04 2022 г.

Начальник методического отдела
_____ Д.Е. Гапеенок
« 27 » 04 2022 г.

Декан факультета ПМиИ
_____ Е.П. Петрунина
« 27 » 04 2022 г.

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

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.

2. ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ[1]

Таблица 2

№	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

[1] 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. 3.

Таблица 3.

Код компетенции	Уровень освоения компетенции	Индикаторы достижения компетенции	Вид учебных занятий[2], работы, формы и методы обучения, способствующие формированию и развитию компетенций[3]	Контролируемые разделы и темы дисциплины[4]	Оценочные средства, используемые для оценки уровня сформированности компетенции[5]	Критерии оценивания результатов обучения
ОПК-4	Знает					
	Недостаточный уровень Оценка «незачтено», «неудовлетворительно»	*ОПК-4.4-1.* 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	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	Текущий контроль – устный опрос.	Не знает значительной части материала курса, не способен самостоятельно выделять главные положения в изученном материале дисциплины

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

[3] 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.

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

[5] 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…

		и причины нарушения компьютерной безопасности.		9. Методы защита программ от изучения и разрушающих программных воздействий (программных закладок и вирусов)		
	Базовый уровень Оценка, «зачтено», «удовлетвори тельно»	*ОПК-4.4-1.* Знает основные методы получения новых знаний с помощью информационн ых технологий для решения задач в области профессиональ ной деятельности с учетом требований информационн ой безопасности; стандарты оформления программной документации и причины нарушения компьютерной безопасности.	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	Текущий контроль – устный опрос.	Знает не менее 50 % основного материала курса, однако испытывает затруднения в его применении

				(программных закладок и вирусов)		
	Средний уровень Оценка «зачтено», «хорошо»	*ОПК-4.4-1.* 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.	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.	Знает основную часть материала курса, способен применить изученный материал на практике, испытывает незначительные затруднения в решении задач
	Высокий уровень Оценка	*ОПК-4.4-1.* Знает основные методы	Лекционные и практические занятия, работа в малых группах,	1. Введение 2. Защита информации от ПЭМИН	Текущий контроль – устный опрос.	Показывает глубокое знание и понимание материала, способен

	«зачтено», «отлично»	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.	интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача экзамена.	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)		применить изученный материал на практике
	Умеет					
	Недостаточный уровень Оценка «незачтено», «неудовлетворительно»	*ОПК-4.4-2.* Умеет применять информационные технологии в практической деятельности и	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка	1. Введение 2. Защита информации от ПЭМИН 3. Основы теории защиты информации в компьютерных системах 4. Основы	Текущий контроль – устный опрос.	Не знает значительной части материала курса, не способен самостоятельно выделять главные положения в изученном материале дисциплины

		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.	и сдача промежуточной аттестации, подготовка и сдача экзамена.	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)		
	Базовый уровень Оценка, «зачтено», «удовлетворительно»	*ОПК-4.4-2.* Умеет применять информационные технологии в практической деятельности и анализировать полученные решения вычислительны	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача экзамена.	10. Введение 11. Защита информации от ПЭМИН 12. Основы теории защиты информации в компьютерных системах 13. Основы криптографии 14. Применение симметричных криптосистем для защиты компьютерной	Текущий контроль – устный опрос.	Умеет воспроизвести не менее 50 % основного материала курса, однако испытывает затруднения при решении практических задач

		х задач; на основе анализа применяемых математически х методов и алгоритмов оценивать эффективность средств защиты информации; ориентироватьс я в современных и перспективных математически х методах защиты информации.		информации 15. Инфраструктура открытых ключей 16. Методы идентификации и аутентификации пользователей компьютерных систем 17. Защита компьютерных систем от удаленных атак через сеть Internet 18. Методы защита программ от изучения и разрушающих программных воздействий (программных закладок и вирусов)		
	Средний уровень Оценка «зачтено», «хорошо»	*ОПК-4.4-2.* Умеет применять информационн ые технологии в практической деятельности и анализировать полученные решения вычислительны х задач; на основе анализа применяемых математически	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	Текущий контроль – устный опрос.	Умеет решать стандартные профессиональные задачи с применением полученных знаний, испытывает незначительные затруднения в решении задач

		х методов и алгоритмов оценивать эффективность средств защиты информации; ориентироваться в современных и перспективных математических методах защиты информации.		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)		
	Высокий уровень Оценка «зачтено», «отлично»	*ОПК-4.4-2.* Умеет применять информационные технологии в практической деятельности и анализировать полученные решения вычислительных задач; на основе анализа применяемых математических методов и	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.	Умеет решать стандартные профессиональные задачи с применением полученных знаний, показывает глубокое знание и понимание материала, способен решить задачу при изменении формулировки

		алгоритмов оценивать эффективность средств защиты информации; ориентироваться в современных и перспективных математических методах защиты информации.		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)		
	Владеет					
	Недостаточный уровень Оценка «незачтено», «неудовлетворительно»	*ОПК-4.4-3.* 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	Текущий контроль – устный опрос.	Не знает значительной части материала курса, не способен самостоятельно выделять главные положения в изученном материале дисциплины

				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)		
	Базовый уровень Оценка, «зачтено», «удовлетворительно»	*ОПК-4.4-3.* 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.	10. Введение 11. Защита информации от ПЭМИН 12. Основы теории защиты информации в компьютерных системах 13. Основы криптографии 14. Применение симметричных криптосистем для защиты компьютерной информации 15. Инфраструктура открытых ключей 16. Методы идентификации и	Текущий контроль – устный опрос.	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.

				аутентификации пользователей компьютерных систем 17. Защита компьютерных систем от удаленных атак через сеть Internet 18. Методы защита программ от изучения и разрушающих программных воздействий (программных закладок и вирусов)		
	Средний уровень Оценка «зачтено», «хорошо»	*ОПК-4.4-3.* 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 аутентификации	Текущий контроль – устный опрос.	Владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности, способен самостоятельно выделять главные положения в изученном материале. Испытывает незначительные затруднения в решении задач.

				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 Оценка «зачтено», «отлично»	*ОПК-4.4-3.* 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 аутентификации пользователей	Текущий контроль – устный опрос.	Свободно владеет навыками теоретического и экспериментального исследования, показывает глубокое знание и понимание изученного материала

				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)		

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

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

Вопросы к экзамену

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.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Содержание изменения	Измененные пункты	Решение Учебно-методического совета