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

КАФЕДРА ЦИФРОВЫХ ТЕХНОЛОГИЙ

УТВЕРЖДАЮ
Проректор по учебно-методической работе
_____ Е.С. Сахарчук
«27» 04 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
Криптография

образовательная программа направления подготовки 01.03.02 "Прикладная математика и информатика"
шифр, наименование

Направленность (профиль)
Вычислительная математика и информационные технологии
Квалификация (степень) выпускника: бакалавр

Форма обучения очная

Курс 4 семестр 8

Москва 2022

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению подготовки 01.03.02 «Прикладная математика и информатика (уровень бакалавриата)», утвержденного приказом Министерства образования и науки Российской Федерации № 9 от 10 января 2018 г. Зарегистрировано в Минюсте России 06 февраля 2018 г. №49937.

Разработчики рабочей программы:

МГГЭУ, заведующий кафедрой цифровых технологий
место работы, занимаемая должность

_____ Митрофанов Е.П. 14.03 20 22 г
подпись Ф.И.О. Дата

Рабочая программа утверждена на заседании кафедры цифровых технологий
(протокол № 4 от « 22 » 03 2022 г.)

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

СОГЛАСОВАНО:

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

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

Заведующий библиотекой
_____В.А. Ахтырская
« 27 » 04 2022 г.

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

Содержание

1. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

1.1. Цели и задачи освоения учебной дисциплины (модуля)

Цель: предполагает формирование у студентов знаний по проблеме криптографической защиты информационных ресурсов, а также практических навыков безопасной работы в информационных системах.

Задачи:

- изучение управления информационными рисками, основных положений построения и функционирования защищенных информационных систем;
- изучение методов и средств комплексной защиты информации в информационных системах коммерческих предприятий и государственных учреждений;
- формирование практических навыков анализа защищенности информационных систем и использования механизмов обеспечения безопасности информации.

1.2. Место дисциплины (модуля) в структуре образовательной программы направления подготовки

Учебная дисциплина «Криптография» относится к части, формируемой участниками образовательных отношений блока Б1. Изучение учебной дисциплины «Криптография» базируется на знаниях, умениях и навыках, полученных обучающимися при изучении дисциплин «Информационная безопасность», «Объектно-ориентированное программирование», «Системное и прикладное программное обеспечение».

Изучение учебной дисциплины «Криптография» необходимо для выполнения выпускной квалификационной работы.

1.3. Требования к результатам освоения учебной дисциплины (модуля)

Процесс освоения учебной дисциплины направлен на формирование у обучающихся следующих компетенций:

Универсальные (УК), общепрофессиональные (ОПК), профессиональные (ПК) – в соответствии с ФГОС 3++.

Код компетенции	Содержание компетенции	Индикаторы достижения компетенции
ПК-7	Способен к разработке и применению алгоритмических и программных решений в области системного и прикладного программного обеспечения	Знает: теоретические основы разработки программных и алгоритмических решений в области системного и прикладного программного обеспечения; математические методы решения задач, процедурный и объектно-ориентированный подходы к разработке информационных систем; актуальные проблемы в области

		программирования; методы и технологии программирования; языки программирования, основы технологии модульного программирования на языках высокого уровня. Умеет: применить математический метод для решения задачи; подобрать рациональную технологию программирования для решения профессиональной задачи; создавать программные продукты и алгоритмические решения в области системного и прикладного программного обеспечения. Владеет: навыками применения математических методов для решения задач и применения стандартных алгоритмов; навыками разработки и создания алгоритмических и программных решений в области системного и прикладного программного обеспечения; навыками разработки программных приложений с использованием современных языков программирования.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

2.1. Объем учебной дисциплины (модуля).

Объем дисциплины «Криптография» составляет 4 зачетных единиц/ 144 часов:

Вид учебной работы	**Всего, часов**	**Очная форма**
		Курс, часов
	Очная форма	4 курс, 8 семестр
Аудиторная работа обучающихся с преподавателем (по видам учебных занятий), всего в том числе:	32	32
Лекции (Л)	8	8
В том числе, практическая подготовка (ЛПП)		
Практические занятия (ПЗ) ***(в том числе зачет)***	24	24
В том числе, практическая подготовка (ПЗПП)	4	4
Лабораторные работы (ЛР)		
В том числе, практическая подготовка (ЛРПП)		
Самостоятельная работа обучающихся (СР)	76	76
В том числе, практическая подготовка (СРПП)	18	18
Промежуточная аттестация (подготовка и сдача), всего:	36	36
Контрольная работа		
Курсовая работа		
Экзамен	36	36
Итого: Общая трудоемкость учебной дисциплины (в часах, зачетных единицах)	144	144

2.2. Содержание разделов учебной дисциплины (модуля)

№ п/п	Наименование раздела (темы)	Содержание раздела (тематика занятий)	Формируемые компетенции (индекс)
1.	Введение в криптографию	Основные понятия, термины, определения. Предмет и задачи дисциплины. Из истории криптографии. Простейшие шифры и их свойства. Шифры замены и перестановки. Композиции шифров. Основные этапы становления криптографии как науки. Характер криптографической деятельности. Открытые сообщения и их характеристики. Виды информации, подлежащие закрытию, их	ПК-7

		модели и свойства. Частотные характеристики открытых сообщений. Критерии на открытый текст. Особенности нетекстовых сообщений. Основные понятия криптографии. Модели шифров. Блочные и поточные шифры. Понятие криптосистемы. Ручные и машинные шифры. Ключевая система шифра. Основные требования к шифрам.	
2.	Шифры перестановки.	Разновидности шифров перестановки: маршрутные, вертикальные перестановки, решетки и лабиринты. Криптоанализ шифров перестановки. Шифры замены. Одноалфавитные и многоалфавитные замены. Вопросы криптоанализа простейших шифров замены. Стандартные алгоритмы криптографической защиты данных. Современные системы шифрования (симметрические и асимметрические). Поточные шифры. Табличное и модульное гаммирование. Случайные и псевдослучайные гаммы. Криптограммы, полученные при повторном использовании ключа. Анализ криптограмм, полученных применением неравновероятной гаммы. Синтез и анализ криптографических алгоритмов: классические шифры, шифры гаммирования и колонной замены.	ПК-7
3.	Имитостойкость шифров	Теоретико-информационный подход к оценке криптостойкости шифров. Криптографическая стойкость шифров. Надежность ключей и сообщений. Совершенные шифры. Безусловно стойкие и вычислительно стойкие шифры. Вопросы практической стойкости. Избыточность языка и расстояние единственности. Имитация и подмена сообщения. Характеристики имитостойкости. Методы обеспечения имитостойкости шифров. Совершенная имитостойкость. Коды аутентификации. Основные методы дешифрования. Помехоустойчивость шифров. Характеристики помехоустойчивости. Характеризация шифров, не размножающих искажений типа замены и пропуска букв.	ПК-7
4.	Реализация криптографических алгоритмов	Основные способы реализация криптографических алгоритмов и требования, предъявляемые к ним. Различие между программными и аппаратными реализациями. Программные реализации шифров. Программно-аппаратная реализация современных криптографических схем и систем. Особенности использования вычислительной техники в криптографии.	ПК-7

		Современные криптографические интерфейсы. Криптографические стандарты. Стандарты систем шифрования (DES, ГОСТ 28147-89). Вопросы синтеза шифров. Сложность криптографических алгоритмов (теорема Кука, пр-полнота). Криптографические протоколы, протоколы с нулевым разглашением. Основные примеры. Связь стойкости протокола со стойкостью базовой криптографической системы. Классификация криптографических протоколов. Электронная цифровая подпись (ЭЦП). Понятие ЭЦП. Стандарты ЭЦП. Однонаправленные функции и методы их построения.	

2.3. Разделы дисциплины и виды занятий

Очная форма обучения

№ п/п	Наименование раздела (темы)	Аудиторная работа		Внеауд. работа	Объем в часах
		Л	ПЗ/ЛР	СР	Всего
		в том числе, ЛПП	в том числе, ПЗПП/ЛРПП	в том числе, СРПП	в том числе, ПП
	РАЗДЕЛ 1. Введение в криптографию				
	1. Основные понятия, термины, определения. Предмет и задачи дисциплины. Из истории криптографии. Простейшие шифры и их свойства. Шифры замены и перестановки. Композиции шифров. Основные этапы становления криптографии как науки. Характер криптографической деятельности. Открытые сообщения и их характеристики. Виды информации, подлежащие закрытию, их модели и свойства. Частотные характеристики открытых сообщений. Критерии на открытый текст. Особенности нетекстовых сообщений. Основные понятия криптографии. Модели	2	6	18	26

	шифров. Блочные и поточные шифры. Понятие криптосистемы. Ручные и машинные шифры. Ключевая система шифра. Основные требования к шифрам.				
	Итого:	2	6	18	26
	В том числе ПП:				14
	РАЗДЕЛ 2. Шифры перестановки.				
	1. Разновидности шифров перестановки: маршрутные, вертикальные перестановки, решетки и лабиринты. Криптоанализ шифров перестановки. Шифры замены. Одноалфавитные и многоалфавитные замены. Вопросы криптоанализа простейших шифров замены. Стандартные алгоритмы криптографической защиты данных. Современные системы шифрования (симметрические и асимметрические). Поточные шифры. Табличное и модульное гаммирование. Случайные и псевдослучайные гаммы. Криптограммы, полученные при повторном использовании ключа. Анализ криптограмм, полученных применением неравновероятной гаммы. Синтез и анализ криптографических алгоритмов: классические шифры, шифры гаммирования и колонной замены.	2	6	18	26
	Итого:	2	6	18	26
	В том числе ПП:				
	РАЗДЕЛ 3. Имитостойкость шифров				
	1. Теоретико-информационный подход к оценке криптостойкости шифров. Криптографическая стойкость шифров. Надежность ключей и сообщений. Совершенные шифры. Безусловно стойкие и вычислительно стойкие шифры. Вопросы практической	2	*6*	20	28

	стойкости. Избыточность языка и расстояние единственности. Имитация и подмена сообщения. Характеристики имитостойкости. Методы обеспечения имитостойкости шифров. Совершенная имитостойкость. Коды аутентификации. Основные методы дешифрования. Помехоустойчивость шифров. Характеристики помехоустойчивости. Характеризация шифров, не размножающих искажений типа замены и пропуска букв.				
	Итого:	2	6	20	28
	В том числе ПП:			8	8
	РАЗДЕЛ 4. Реализация криптографических алгоритмов				
	1. Основные способы реализация криптографических алгоритмов и требования, предъявляемые к ним. Различие между программными и аппаратными реализациями. Программные реализации шифров. Программно-аппаратная реализация современных криптографических схем и систем. Особенности использования вычислительной техники в криптографии. Современные криптографические интерфейсы. Криптографические стандарты. Стандарты систем шифрования (DES, ГОСТ 28147-89). Вопросы синтеза шифров. Сложность криптографических алгоритмов (теорема Кука, np-полнота). Криптографические протоколы, протоколы с нулевым разглашением. Основные примеры. Связь стойкости протокола со стойкостью базовой криптографической системы. Классификация криптографических	2	6	20	28

	протоколов. Электронная цифровая подпись (ЭЦП). Понятие ЭЦП. Стандарты ЭЦП. Однонаправленные функции и методы их построения.				
	Итого:	2	6	20	28
	В том числе ПП:		4	10	14
	Всего:	8	24	76	108
	В том числе ПП:		4	18	22

2.4. План самостоятельной работы обучающегося по дисциплине (модулю)

Очная форма обучения

№	Название разделов и тем	Виды самостоятельной работы	Трудоемкость (часов)	Формируемые компетенции	Формы контроля
1.	Введение в криптографию	Самоподготовка Самостоятельное изучение разделов	18	ПК-7	Устный опрос, проверка задания
2.	Шифры перестановки.	Самоподготовка Самостоятельное изучение разделов	18	ПК-7	Устный опрос, проверка задания
3.	Имитостойкость шифров	Самоподготовка Самостоятельное изучение разделов	20	ПК-7	Устный опрос, проверка задания
4.	Реализация криптографических алгоритмов	Самоподготовка Самостоятельное изучение разделов	20	ПК-7	Устный опрос, проверка задания
		Экзамен	76		Экзамен

3. ОСОБЕННОСТИ ОБУЧЕНИЯ ИНВАЛИДОВ И ЛИЦ С ОВЗ

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 экзамену. Подготовка к экзамену 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, проверка задания.
Промежуточная аттестация – экзамен.

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

не предусмотрено

6.3. Курсовая работа

не предусмотрено учебным планом.

6.4. Вопросы к зачету

не предусмотрено учебным планом.

6.5. Вопросы к экзамену

1. Симметричное шифрование. Принцип Керкгофса.
2. Примеры применения криптографии. Классы атак.
3. Подстановочный шифр и его взлом.
4. Шифр Виженера, роторная машина.
5. Определение шифра. Шифр Вернама и совершенная секретность.
6. Вероятностные переформулировки совершенной секретности.
7. Эксперимент по взлому. Длина ключа в случае совершенной секретности.
8. Псевдослучайный генератор и его предсказуемость. Линейный конгруэнтный генератор.
9. Атаки на потоковые шифры.
10. Статистические тесты, преимущество. Надежность псевдослучайного генератора.
11. Непредсказуемость надежного генератора. Вычислительная неразличимость.
12. Определение схемы шифрования с закрытым ключом. Вычислительная стойкость.
13. Стойкость потокового шифра. Шифрование нескольких сообщений.
14. Стойкость относительно chosen plaintext-атак. Функции с ключом и псевдослучайные функции.
15. Шифрование с помощью псевдослучайной функции и его устойчивость.
16. Псевдослучайные перестановки. Методы работы блочных шифров.
17. Конструкции псевдослучайных перестановок. Сеть Фейстеля.
18. Аутентификация сообщений. Код аутентификации сообщений и его надежность.
19. Конструкция кода аутентификации сообщений из псевдослучайной функции.
20. Протокол интерактивного обмена ключами, его надежность. Описание протокола Диффи–Хеллмана.
21. Задача DDH и надежность протокола Диффи–Хеллмана.
22. Схема шифрования с открытым ключом, ее надежность относительно подслушивания и относительно chosen plaintext-атак.
23. Шифрование нескольких сообщений, его надежность. Гибридное шифрование.
24. Наивная схема шифрования RSA. Ускорение дешифровки, маленький показатель.
25. RSA с набивкой, задача RSA и надежность схемы шифрования RSA с набивкой.
26. Схема Эль-Гамаля и ее надежность.
27. Квадратичные вычеты и символ Якоби.
28. Задача определения квадратичных вычетов и схема шифрования Гольдвассер–Микали.
29. Извлечение квадратных корней и схема шифрования Рабина.
30. Остатки по модулю N2 и схема шифрования Пайе.
31. Схема цифровой подписи, ее надежность. Наивная схема RSA.
32. RSA с хэшем. Схема одноразовой подписи Лэмпорта.
33. Доказательства с нулевым разглашением.

34. Сертификаты. Схемы разделения секрета.

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

7.1. Основная литература

1. Криптографическая защита информации : учебное пособие / С. О. Крамаров, О. Ю. Митясова, С. В. Соколов [и др.] ; под ред. С. О. Крамарова. — Москва : РИОР : ИНФРА-М, 2021. — 321 с. — (Высшее образование). - ISBN 978-5-369-01716-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1153156
2. Бабаш, А. В. История защиты информации в зарубежных странах : учебное пособие / А.В. Бабаш, Д.А. Ларин. — Москва : РИОР : ИНФРА-М, 2021. — 284 с. — (Высшее образование). — DOI: https://doi.org/10.12737/15090. - ISBN 978-5-369-01844-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1215133
3. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2021. — 400 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1210523
4. Романьков, В. А. Введение в криптографию : курс лекций / В.А. Романьков. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 240 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-00091-493-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1514566

7.2. Дополнительная литература

1. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2021. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/469567
2. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2021. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/470279
3. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2021. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/469758

7.3. Программное обеспечение

Сетевой компьютерный класс, оснащенный современной техникой

1. Офисный программный пакет (например, Microsoft Office 2007 или более поздних версий).
2. Web-браузер Mozilla Firefox или Google Chrome
3. 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

7.5. Методические указания и материалы по видам занятий

1. Автоматика и Телемеханика / Automation and Remote.
2. Автоматика, связь, информатика.
3. Безопасность информационных технологий.
4. Бизнес-информатика.
5. Вестник кибернетики (электронный журнал).
6. Вестник компьютерных и информационных технологий.
7. Вопросы защиты информации.
8. Вопросы кибербезопасности.
9. Геоинформатика/Geoinformatika.
10. Информатизация образования и науки.
11. Информатизация и связь.
12. Информатика и ее применения.
13. Информатика и образование.
14. Информатика и системы управления.
15. Информационное общество.
16. Информационное право.
17. Информационно-измерительные и управляющие системы.
18. Информационно-управляющие системы.
19. Информационные ресурсы России.
20. Информационные системы и технологии.
21. Информационные и телекоммуникационные технологии.
22. Информационные технологии.
23. Информационные технологии в проектировании и производстве.
24. Информационные технологии и вычислительные системы.
25. Информация и безопасность.
26. Информация и космос.
27. Компьютерная оптика.
28. Компьютерные инструменты в образовании.
29. Компьютерные исследования и моделирование.
30. Математическая биология и биоинформатика (электронное научное издание).

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	Содержание изменения	Измененные пункты	Решение Учебно-методического совета