ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ИНКЛЮЗИВНОГО ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО - ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»

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

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 041CD9B1001CAF77894D606F5F479EB1E9
Владелец: Сахарчук Елена Сергеевна
Действителен: с 26.09.2022 до 26.09.2023

УТВЕРЖДАЮ

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

«31» августа 2021г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) КРИПТОГРАФИЯ

образовательная программа направления подготовки
09.03.01 "Информатика и вычислительная техника"
Блок Б.1.О.26 «Дисциплины (модули)», обязательная часть

Профиль подготовки
Программное обеспечение вычислительной техники и информационных систем

Квалификация (степень) выпускника
Бакалавр

Форма обучения: очная
Курс 3 семестр 6

Москва
2021

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования направления подготовки 09.03.01 **Информатика и вычислительная техника**, утвержденного приказом Министерства образования и науки Российской Федерации № 929 от 19 сентября 2017 г.

Составители рабочей программы: ____МГГЭУ, доцент кафедры ПМиИ по областям _
место работы, занимаемая должность

«30» августа 2021 г. _____ Е.В. Петрунина
Дата подпись Ф.И.О.

Рецензент: МГГЭУ, доцент кафедры информационных технологий и прикладной математики_____
место работы, занимаемая должность

_____ Белоглазов А.А. «30» августа 2021 г.
подпись Ф.И.О. Дата

Рабочая программа утверждена на заседании кафедры Информационных технологий и прикладной математики (протокол № 2 от «30» августа 2021 г.)

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

СОГЛАСОВАНО
Начальник
учебного отдела

«30» августа 2021 г. _____ И.Г.Дмитриева
Дата подпись Ф.И.О.

СОГЛАСОВАНО
Декан факультета ПМиИ

«30» августа 2021 г. _____ Е.В. Петрунина
Дата подпись Ф.И.О.

СОГЛАСОВАНО
Заведующая библиотекой

«30» августа 2021 г. _____ В.А. Ахтырская
Дата подпись Ф.И.О.

Содержание

1. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

1.1. Цели и задачи изучения дисциплины

Цели дисциплины:

- формирование у студентов системных взглядов на управление информационными рисками, на обеспечение комплексной безопасности информационных систем, а также практических навыков безопасной работы в информационных системах.

Задачи дисциплины:

- изучение основ 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 вариативной части блока «Дисциплин (модулей)» Б1. Изучение учебной дисциплины «Криптография» базируется на знаниях, умениях и навыках, полученных студентами при изучении дисциплин: Математика», «Информатика», «Операционные системы», «Вычислительные системы, сети и телекоммуникации».

Изучение учебной дисциплины необходимо для освоения таких дисциплин, как «Высокопроизводительные вычисления», «Теория формальных языков и методов компиляции», и производственной практики «Практика по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности».

1.3. Требования к результатам освоения учебной дисциплины (модуля)

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

Код компетенции	Содержание компетенции	Индикаторы достижения компетенции
ОПК-1	Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности	ОПК-1.1. Знать: основы математики, физики, вычислительной техники и программирования ОПК-1.2. Уметь: решать стандартные профессиональные задачи с применением естественнонаучных и общеинженерных знаний, методов математического анализа и моделирования. ОПК-1.3. Владеть: навыками теоретического и экспериментального исследования объектов профессиональной деятельности

ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. ОПК-3.3. Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

2.1. Объём учебной дисциплины(модуля).

Объём дисциплины «Информационные технологии в профессиональной деятельности» составляет 6 зачётных единиц/216 часов:

Вид учебной работы	**Всего, часов**	**Очная форма**
		Курс, часов
	Очная форма	**3 курс**
		6 сем
Аудиторная работа обучающихся с преподавателем (по видам учебных занятий), всего в том числе:	72	72
Лекции (Л)	22	22
Практические занятия (ПЗ)	50	50
В том числе, практическая подготовка (ПЗПП)		
Лабораторные работы (ЛР)		
В том числе, практическая подготовка (ЛРПП)		
Самостоятельная работа обучающихся (СР)	72	72
В том числе, практическая подготовка (СРПП)		
Промежуточная аттестация (подготовка и сдача), всего:		
Контрольная работа	36	36
Курсовая работа		
Зачет		
Экзамен		экзамен
Итого: Общая трудоемкость учебной дисциплины (в часах, зачетных единицах)	180 (5 з.е)	180 (5 з.е)

2.2. Содержание дисциплины по темам (разделам)

№ раздела	Наименование раздела, тема	Содержание раздела	Форма текущего контроля
1	История и основные направления развития современной защитой информации	Важные моменты в истории развития теории защиты информации. «Наивная» криптография: шифр Цезаря, шифр Пиблса; Формальная криптография: шифр Вижинера, роторные криптосистемы; математическая криптография: доказуемо криптостойкие системы; компьютерная криптография: криптосистемы с открытым ключом, автоматизированный криптоанализ.	Устный опрос
2	Криптография с открытым ключом	Модель передачи сообщения в криптосистеме с открытым ключом. Основы теории чисел: функция Эйлера, обобщенный алгоритм Евклида, быстрый алгоритм возведения в степень справа налево и слева направо. Понятие односторонней функции. Примеры односторонних функций. Система защищенной передачи ключей Диффи и Хеллмана. Шифр Шамира. Шифр Эль-Гамаля. Шифр RSA. Электронная подпись на базе RSA.	Устный опрос, контрольная работа
3	Криптографические протоколы	Понятие риптографического протокола. Протокол «Ментальный покер». Протокол «Доказательство с нулевым знанием»: задача о раскраске, задача о гамильтоновом цикле. Электронные деньги. Задача о взаимной верификации.	Устный опрос, контрольная работа
4	Шифры с секретным ключом	Первый шифр с секретным ключом: шифр Цезаря. Понятие блокового шифра. Шифр ГОСТ 28147-89. Шифр RC-5. Шифр RC-6. Шифр AES (Rijndael). Режимы функционирования блоковых шифров: режим электронной кодовой книги (ECB)	Устный опрос, тестирование

2.3 Разделы дисциплин и виды занятий
Очная форма обучения

№ п/п	Наименование раздела	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
1	История и основные направления развития современной защитой информации	6	12	18	36
2	Криптография с открытым ключом	6	14	18	38
3	Криптографические протоколы	6	12	18	36
4	Шифры с секретным ключом	4	12	18	36
	Итого:	22	*50*	72	144

2.4. Планы теоретических (лекционных) занятий
Очная форма обучения

№	Наименование тем лекций	Кол-во часов во 2 семестре по видам работы	
		Л	в том числе, ЛПП
	2 семестр		
РАЗДЕЛ 1. История и основные направления развития современной защитой информации		4	
РАЗДЕЛ 2. Криптография с открытым ключом		4	
РАЗДЕЛ 3. Криптографические протоколы		4	
РАЗДЕЛ 4. Шифры с секретным ключом		4	

2.5. Планы практических (семинарских) занятий

Очная форма обучения

№	Наименование тем лекций	Кол-во часов во 2 семестре по видам работы	
		П	в том числе, ПЗПП
	2 семестр		
РАЗДЕЛ 1. История и основные направления развития современной защитой информации		12	
РАЗДЕЛ 2. Криптография с открытым ключом		14	
РАЗДЕЛ 3. Криптографические протоколы		12	
РАЗДЕЛ 4. Шифры с секретным ключом		12	

2.6. Планы лабораторных работ – не предусмотрены учебным планом

2.7. Планы самостоятельной работы обучающегося по дисциплине (модулю)

№	Название разделов и тем	Виды самостоятельной работы	Трудоемкость	Формируемые компетенции	Формы контроля
1.	История и основные направления развития современной защитой информации	Цели и задачи криптоанализа. Криптографическая устойчивость информационных систем.	18	ОПК-1, ОПК-3	Устный опрос
2.	Криптография с открытым ключом	Самостоятельная работа студента	18	ОПК-1, ОПК-3	Устный опрос
3.	Криптографические протоколы	Модель передачи скрытых сообщений. Первые стеганографические системы. Современная стеганография. Защита авторского права. Цифровые водяные знаки. Цифровые отпечатки пальцев.	18	ОПК-1, ОПК-3	Устный опрос
4.	Шифры с секретным ключом	Обнаружение факта передачи скрытого сообщения. Понятие идеальной стеганографической системы.	18	ОПК-1, ОПК-3	Устный опрос

2.8. Планы практической подготовки – не предусмотрены учебным планом

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.

3. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

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

Самостоятельная работа в рамках образовательного процесса решает следующие задачи:

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

Основными принципами организации самостоятельной работы являются:

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

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

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

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

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

- изучение конспектов лекций, раскрывающих материал, знание которого проверяется контрольной работой;

− повторение учебного материала, полученного при подготовке к практическим занятиям и во время их проведения;

− изучение дополнительной литературы, в которой конкретизируется содержание проверяемых знаний.

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

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

Подготовка к зачету с оценкой. Подготовка к зачету с оценкой 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 зачетом. 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.

4. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Интерактивные образовательные технологии, используемые в аудиторных занятиях и самостоятельной работе обучающихся

Семестр	Вид занятия (Л, ПР, ЛР)	Используемые интерактивные образовательные технологии	Количество часов
5	Л	Проблемная лекция, лекция-визуализация, лекция-диалог	22
	ПР	Ситуационный анализ, дискуссия, круглый стол	50
Итого:			72

5. 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, контрольные работы, тестирование.

Промежуточная аттестация – экзамен.

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

6.3. Курсовая работа – не предусмотрено.

6.4. Вопросы к экзамену

1. Основные этапы развития теории защиты информации.
2. Наивная криптография. Шифр Цезаря.
3. Идеальная криптосистема. Шифр Вернама.
4. Система обмена ключами Диффи и Хеллмана.
5. Шифр Шамира.
6. Шифр Эль-Гамаля.
7. Шифр RSA.
8. Электронная цифровая подпись. Схема протокола. Пример построения на основе шифра RSA.
9. Криптосистемы на эллиптических кривых.
10. Основы арифметики на эллиптических кривых.
11. Принцип построения криптосистем на эллиптических кривых.
12. Генераторы псевдослучайных чисел
13. Потоковые шифры. Примеры потоковых шифров.
14. Шифр RC4.
15. Блоковые шифры.
16. Примеры блоковых шифров. Режимы функционирования блоковых шифров.
17. Схема построения потокового шифра на основе блокового шифра.
18. Теорема Шеннона.
19. Расстояние Хемминга. Вес Хэмминга. Код Хэмминнга.
20. Линейные коды. Проверочная матрица. Порождающая матрица.
21. Теорема и связи проверочной и порождающей матриц.
22. Циклические коды.
23. Границы объемов кодов. Граница Хэмминга. Граница Синглтона.
24. Симметричные алгоритмы шифрования.
25. Ассиметричные алгоритмы шифрования.
26. Биометрические методы идентификации.
27. Модели разграничения доступа.
28. Модель передачи скрытых сообщений.
29. Первые стеганографические системы. Современная стеганография.
30. Защита авторского права. Цифровые водяные знаки. Цифровые отпечатки пальцев.

6.6. Контроль освоения компетенций

Вид контроля	Контролируемые темы (разделы)	Компетенции, компоненты которых контролируются

6. 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

1. Сетевой компьютерный класс, оснащенный современной техникой
2. Офисный программный пакет (например, Microsoft Office 2003 или более поздних версий).
3. Web-браузер Mozilla Firefox или Google Chrome
4. Экран для проектора.

7.4. Электронные ресурсы

1. Национальный открытый университет ИНТУИТ [Электронный ресурс]. URL: http://www.intuit.ru
2. Хабрахабр [Электронный ресурс]. URL: http://habrahabr.ru/
3. 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

7.5Методические указания и материалы по видам занятий

1.Электронная библиотека РГБ. https://www.rsl.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий	Перечень оборудования и технических средств обучения
1	Аудитория №402	11 компьютеров Системный блок 1: Процессор Intel(R) Core(TM) i5-4570 CPU @ 3.20GHz 8192 ОЗУ HDD Объем: 500 ГБ Монитор Benq G922HDA- 22 дюйма Системный блок 2: Процессор Intel(R) Core(TM) i5-4170 CPU @ 3.70GHz 4096 МБ ОЗУ; HDD Объем: 500 ГБ Монитор DELL 178FP Системный блок 3: Процессор Intel(R) Core(TM) i3-6100 CPU @ 3.70GHz 4096 МБ ОЗУ; SSD Объем: 120 ГБ Монитор Samsung 940NW Акустическая система 2.0 Интерактивная доска Smart Board Проектор Epson EH-TW535W
2	Аудитория №403	Системный блок: Процессор Intel® Pentium®Dual-Core E2180 2048 ОЗУ; 320 HDD Монитор AOC 2470W Проектор Epson EH-TW5300 с акустической системой
3	Аудитория №405	Системный блок: Процессор Intel® Pentium®Dual-Core E2180 2048 ОЗУ; 320 HDD Монитор AOC 2470W Проектор Epson EH-TW5300 с акустической системой
4	Аудитория №302	11 компьютеров Системный блок: Процессор Intel(R) Core(TM) i3-2100 CPU @ 3.10GHz 4096 МБ ОЗУ; HDD Объем: 320 ГБ Монитор Acer P206HL - 20 дюймов Акустическая система Sven Интерактивная доска Smart Board Проектор Epson EH-TW535W
5	Аудитория №303	Системный блок: Процессор Intel® Pentium®Dual-Core E5200 2048 ОЗУ; 320 HDD Монитор Samsung SyncMaster 940NW Акустическая система Sven Проектор Nec M260W
6	Аудитория №305	Системный блок: Процессор Intel® Core™2 Duo E8500 2048 ОЗУ; 250 HDD Монитор Samsung SyncMaster 940NW Акустическая система Sven

		Проектор Nec M260W
7	Аудитория №306	12 компьютеров Системный блок: Процессор Intel(R) Core(TM) i5-2400 CPU @ 3.10GHz 8192 ОЗУ; HDD Объем: 500 ГБ Монитор DELL EX231W - 24 дюйма Интерактивная доска Elite Panaboard UB-T880W с акустической системой Проектор Epson EB-440W
8	Аудитория №308	Системный блок: Процессор Intel(R) Core(TM) i5-2400 CPU @ 3.10GHz; 8192 ОЗУ HDD Объем: 500 ГБ Монитор DELL EX231W - 24 дюйма Интерактивная доска Elite Panaboard UB-T880W с акустической системой Проектор Epson EB-440W
9	Аудитория №2-120	Системный блок: Процессор Intel® Core™2 Duo E8500 2048 ОЗУ$ 250 HDD Монитор Samsung SyncMaster 940NW Акустическая система Sven Проектор Nec M260W
10	Аудитория №109	11 компьютеров Системный блок: Процессор Intel(R) Core(TM) i5-6400 CPU @ 2.70GHz 4096 МБ ОЗУ SSD Объем: 120 ГБ Монитор Philips PHL 243V5 - 24 дюйма Акустическая система Sven Интерактивная доска Smart Board Проектор Epson EH-TW535W
11	Аудитории № 309, 310, 311, 410, 411	Проектор переносной Epson EB-5350 (1080p)– 1 шт. Экран переносной Digis 180x180 – 1 шт. Ноутбук HP ProBook 640 G3 (Intel Core i5 7200U, 4gb RAM, 250 SSD) – 1 шт.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

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