Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный университет им. А.Н. Косыгина
(Технологии. Дизайн. Искусство)»

Институт Мехатроники и робототехники

Кафедра Автоматика и промышленная электроника

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Основы информационной безопасности

Уровень образования	бакалавриат
Направление подготовки	09.03.01 Информатика и вычислительная техника
Направленность (профиль)	Сквозные технологии и искусственный интеллект
Срок освоения образовательной программы по очной форме обучения	4 года
Форма обучения	очная

Рабочая программа учебной дисциплины «Основы информационной безопасности» основной профессиональной образовательной программы высшего образования, рассмотрена и одобрена на заседании кафедры, протокол № 10 от 07.03.2024 г.

Разработчик рабочей программы учебной дисциплины:

1. Доцент А.А. Казначеева

Заведующий кафедрой: Е.А. Рыжкова

1. ОБЩИЕ СВЕДЕНИЯ

Учебная дисциплина «Основы информационной безопасности» изучается в первом семестре.
Курсовая работа/Курсовой проект – не предусмотрен(а)

1.1. Форма промежуточной аттестации:

Экзамен.

1.2. Место учебной дисциплины в структуре ОПОП

Учебная дисциплина «Основы информационной безопасности» относится к обязательной части программы.
Результаты обучения по учебной дисциплине, используются при изучении следующих дисциплин и прохождения практик:

– Информационные и коммуникационные технологии в профессиональной деятельности;
– Базы данных;
– Цифровые технологии в управлении;
– Цифровое производство.

Результаты освоения учебной дисциплины в дальнейшем будут использованы при прохождении учебной практики и выполнении выпускной квалификационной работы.

2. ЦЕЛИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Современный специалист в области информационных технологий должен обладать знаниями и навыками обеспечения информационной безопасности. Связано это с тем, что в информационных системах предприятий и организаций хранится и обрабатывается критически важная информация, нарушение конфиденциальности, целостности или доступности которой может привести к нежелательным последствиям. Поэтому вопросам обеспечения информационной безопасности должно уделяться внимание на всех этапах разработки и эксплуатации информационных систем.

Целями изучения дисциплины «Основы информационной безопасности» являются:

– изучение базовых понятий, связанных с обеспечением информационной безопасности: виды основных угроз и меры противодействия им;

– изучение основных понятий криптографии: алгоритмы симметричного и ассиметричного шифрования, процесс создания инфраструктуры открытых ключей; хещ-функции;

– изучение протоколов криптографической защиты данных, передаваемых по телекоммуникационным сетям, использующим стек протоколов TCP/IP, использование межсетевых экранов для защиты сетей;

– рассмотрение современных методик анализа и управления рисками, связанными с информационной безопасностью.

2.1. Формируемые компетенции, индикаторы достижения компетенций, соотнесённые с планируемыми результатами обучения по дисциплине:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине
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	ИД-ОПКК-3.1 Использование методов поиска и анализа информации для подготовки документов на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий, с учетом соблюдения авторского права и требований информационной безопасности	– Применяет логико-методологический инструментарий для критической оценки получаемой информации и выбирает оптимальное решение поставленной задачи на основе системного подхода.
	ИД-ОПК-3.3 Соблюдение требований по информационной безопасности	– Владеет сутью общенаучных и конкретно-научных методов и принципов исследования. – Владеет базовыми понятиями, связанными с обеспечением информационной безопасности, видами основных угроз и мерами противодействия им. – Применяет методы и алгоритмы симметричного и ассиметричного шифрования данных.
	ИД-ОПК-3.4 Использование современных информационно-коммуникационных технологий для решения стандартных задач профессиональной деятельности.	– Использует математический аппарат и цифровые информационные технологии (программы SMath Solver, Excel) для сбора и обработки данных необходимых для анализа и постановки задачи цифровизации технологических процессов; использует цифровые сертификаты. – Использует протоколы крипто-графической защиты данных, передаваемых по телекоммуникацион-ным сетям, использующим стек протоколов TCP/IP, межсетевые экраны для защиты сетей.
ОПК-4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	ИД-ОПК-4.2 Разработка специальной (технической) документации по проектируемым информационным системам в соответствии со стандартами, нормами и правилами	– Применяет навыки работы с нормативной документацией на электронных ресурсах Консультант, Гарант, Каталог ГОСТ www.internet-law, в поисковых системах Web of Science, PatSearch и базах данных Global Patent Index для оформления прав интеллектуальной собственности на научные разработки в сфере цифровых технологий.

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине
	ИД-ОПК-4.3 Разработка инструкций для пользователей информационных и автоматизированных систем	– Владеет современными методиками анализа и управления рисками, связанными с информационной безопасностью; – Владеет современными методиками по разработке инструкций для специалистов в области применения современных информационных систем: руководства системного программиста, программиста, пользователя.

3. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Общая трудоёмкость учебной дисциплины по учебному плану составляет:

по очной форме обучения –	5	**з.е.**	160	**час.**

3.1. Структура учебной дисциплины для обучающихся по видам занятий

Структура и объем дисциплины									
Объем дисциплины по семестрам	**форма промежуточной аттестации**	**всего, час**	**Контактная аудиторная работа, час**				**Самостоятельная работа обучающегося, час**		
			лекции, час	**практические занятия, час**	**лабораторные занятия, час**	**практическая подготовка, час**	***курсовая работа/ курсовой проект***	**самостоятельная работа обучающегося,**	**промежуточная аттестация, час**
1 семестр	Экзамен	160	34	34				60	32
Всего:		160	34	34				60	32

3.2. Структура учебной дисциплины для обучающихся по разделам и темам дисциплины: (очная форма обучения)

Планируемые (контролируемые) результаты освоения: коды формируемых компетенций и индикаторов достижения компетенций	Наименование разделов, тем; формы промежуточной аттестации	Виды учебной работы				Самостоятельная работа, час	Виды и формы контрольных мероприятий, обеспечивающие по совокупности текущий контроль успеваемости; формы промежуточного контроля успеваемости
		Контактная работа					
		Лекции, час	Практические занятия, час	Лабораторные работы/ индивидуальные	Практическая подготовка, час		
ОПК-3: ИД-ОПК-3.1 ИД-ОПК-3.3 ИД-ОПК-3.4 ОПК-4: ИД-ОПК-4.2 ИД-ОПК-4.3	**Раздел I. Теоретические основы информационной безопасности**	**4**	**6**	**x**	**x**	**10**	
	Тема 1.1 Информация и ее свойства. Общая схема процесса обеспечения информационной безопасности. Средства обеспечения защиты: идентификация, аутентификация, управление доступом.	2				4	Формы текущего контроля по разделу I: 1. Входной контроль знаний (устный опрос). 2. Разбор теоретического материала в формате устной дискуссии. 3. Выполнение практических работ. 4. Контрольное тестирование.
	Тема 1.2 Способы передачи конфиденциальной информации на расстоянии. Криптография и ее основные понятия. Криптоанализ.	2				2	
	Практическое занятие № 1.1 Использование цифровых сертификатов.		2			2	
	Практическое занятие № 1.2 Задачи на тему: теоретико-числовые методы в криптографии.		4			2	
ОПК-3: ИД-ОПК-3.1 ИД-ОПК-3.3 ИД-ОПК-3.4 ОПК-4: ИД-ОПК-4.2 ИД-ОПК-4.3	**Раздел II. Криптографические методы защиты информации**	**14**	**14**	**x**	**x**	**10**	
	Тема 2.1 История криптографии в России.	2				1	Формы текущего контроля по разделу II: 1. Входной контроль знаний (устный опрос). 2. Разбор теоретического материала в формате устной дискуссии. 3. Выполнение практических работ.
	Тема 2.2 Классификация шифров. Шифрование с закрытым ключом. Поточные и блочные шифры на основе схемы Фейстеля и SP-сети.	4				1	
	Тема 2.3	4				1	

Планируемые (контролируемые) результаты освоения: коды формируемых компетенций и индикаторов достижения компетенций	Наименование разделов, тем; формы промежуточной аттестации	Виды учебной работы				Самостоятельная работа, час	Виды и формы контрольных мероприятий, обеспечивающие по совокупности текущий контроль успеваемости; формы промежуточного контроля успеваемости
		Контактная работа					
		Лекции, час	Практические занятия, час	Лабораторные работы/ индивидуальные	Практическая подготовка, час		
	Ассиметричная криптография. Шифрование с открытым ключом. Протокол Диффи-Хеллмана. Хеш-функции и их свойства.						4. Контрольное тестирование.
	Тема 2.4 Инфраструктура открытых ключей. Цифровые сертификаты. Электронная цифровая подпись.	4				1	
	Практическое занятие № 2.1 Шифры замены и перестановки. Модели шифров. Гаммирование.		4			1	
	Практическое занятие № 2.2 Симметричное шифрование данных. Реализация таблицы Вижинера средствами Ms EXCEL.		2			1	
	Практическое занятие № 2.3 Схемы разделения секрета. Ассиметричные шифры RSA и Эль-Гамаля. Хеширование.		4			2	
	Практическое занятие № 2.4 Алгоритмы электронно-цифровой подписи.		4			2	
ОПК-3: ИД-ОПК-3.1 ИД-ОПК-3.3 ИД-ОПК-3.4 ОПК-4: ИД-ОПК-4.2 ИД-ОПК-4.3	**Раздел III. Защита информации в IP-сетях**	**14**	**6**	**x**	**x**	**10**	Формы текущего контроля по разделу III: 1. Входной контроль знаний (устный опрос). 2. Разбор теоретического материала в формате устной дискуссии. 3. Выполнение практических работ. 4. Контрольное тестирование.
	Тема 3.1 Информационная безопасность пользователя. Парольные системы аутентификации.	2				1	
	Тема 3.2 Основные понятия локальных и глобальных компьютерных сетей. Информационная безопасность в Интернете. Протокол защиты электронной почты S/MIME.	4				1	

Планируемые (контролируемые) результаты освоения: коды формируемых компетенций и индикаторов достижения компетенций	Наименование разделов, тем; формы промежуточной аттестации	Виды учебной работы				Самостоятельная работа, час	Виды и формы контрольных мероприятий, обеспечивающие по совокупности текущий контроль успеваемости; формы промежуточного контроля успеваемости
		Контактная работа					
		Лекции, час	Практические занятия, час	Лабораторные работы/ индивидуальные	Практическая подготовка, час		
	Тема 3.3 Протоколы передачи данных SSL и TLS. Параметры их безопасности.	4				1	
	Тема 3.4 Протоколы семейства IPSec: история, архитектура, подключение. Межсетевые экраны и их типы.	4				1	
	Практическое занятие № 3.1 Управление доступом в СУБД SQL Server.		2			2	
	Практическое занятие № 3.2 Создание центра сертификации (удостоверяющего центра) в Windows Server 2008.		2			2	
	Практическое занятие № 3.3 Встроенный межсетевой экран Windows Server 2008.		2			2	
ОПК-3: ИД-ОПК-3.1 ИД-ОПК-3.3 ИД-ОПК-3.4 ОПК-4: ИД-ОПК-4.2 ИД-ОПК-4.3	**Раздел IV. Анализ и управление рисками в сфере информационной безопасности**	**2**	**8**	**x**	**x**	**12**	
	Тема 4.1 Введение в проблему. Управление рисками.	0,5				2	Формы текущего контроля по разделу IV:[1] 1. Входной контроль знаний (устный опрос). 2. Разбор теоретического материала в формате устной дискуссии. 3. Выполнение практических работ.
	Тема 4.2 Методики построения систем защиты информации.	0,5				2	
	Тема 4.3 Методики и программные продукты для оценки рисков.	1				2	
	Практическое занятие № 4.1		2			2	

Планируемые (контролируемые) результаты освоения: коды формируемых компетенций и индикаторов достижения компетенций	Наименование разделов, тем; формы промежуточной аттестации	Виды учебной работы				Самостоятельная работа, час	Виды и формы контрольных мероприятий, обеспечивающие по совокупности текущий контроль успеваемости; формы промежуточного контроля успеваемости
		Контактная работа					
		Лекции, час	Практические занятия, час	Лабораторные работы/ индивидуальные	Практическая подготовка, час		
	Установка Avast Free Antivirus. Развертывание антивирусной защиты: установка агентов администрирования, проверка совместимости.						4. Контрольное тестирование.
	Практическое занятие № 4.2 Работа с вирусными инцидентами.		2			2	
	Практическое занятие № 4.3 Настройка протокола IPSec в Windows Server.		4			2	
	Экзамен.	x	x	x	x	18	Экзамен по билетам
	ИТОГО за первый семестр	**34**	**34**			**60**	
	ИТОГО за весь период	**34**	**34**			**60**	

3.3. Краткое содержание учебной дисциплины

№ пп	Наименование раздела и темы дисциплины	Содержание раздела (темы)
Раздел I	**Теоретические основы информационной безопасности**	
Тема 1.1	Информация и ее свойства. Общая схема процесса обеспечения информационной безопасности. Средства обеспечения защиты: идентификация, аутентификация, управление доступом.	Понятие информации и ее свойства. Концепция информационной безопасности. Угрозы безопасности и направления ее защиты. Методы аутентификации. Процесс построения и оценки системы обеспечения безопасности. Стандарт ISO/IEC 15408. Математические методы защиты информации и их основы.
Тема 1.2	Способы передачи конфиденциальной информации на расстоянии. Криптография и ее основные понятия. Криптоанализ.	Основные задачи криптографии. Правило стойкости шифр системы. Математическая модель процессов шифрования и дешифрования. Классификация шифров. Основные понятия криптоанализа.
Раздел II	**Криптографические методы защиты информации**	
Тема 2.1	История криптографии в России.	Появление криптографии в России. Период становления советской криптографии. Современный подход.
Тема 2.2	Классификация шифров. Шифрование с закрытым ключом. Поточные и блочные шифры на основе схемы Фейстеля и SP-сети.	Симметричная криптография и ее преимущества. Требования к поточному блочному алгоритмам шифрования. Алгоритмы DES, AES, ГОСТ-28147-89, CAST-128, KeeLog, Present.
Тема 2.3	Ассиметричная криптография. Шифрование с открытым ключом. Протокол Диффи-Хеллмана. Хеш-функции и их свойства.	Основные понятия. Распределение ключей по схеме Диффи-Хеллмана. Криптографические системы RSA и Эль-Гамаля. Совместное использование симметричных и ассиметричных шифров. Хеш-функции без ключа и с ключом. Алгоритмы семейств MD, SHA, ГОСТ Р 34.11-2012.
Тема 2.4	Инфраструктура открытых ключей. Цифровые сертификаты. Электронная цифровая подпись.	Атака типа man in the middle. Иерархия центров сертификации и клиентов. Сертификаты и электронно-цифровая подпись.
Раздел III	**Защита информации в IP-сетях**	
Тема 3.1	Информационная безопасность пользователя. Парольные системы аутентификации.	Понятие фишинга. Парольная защита данных на основе комбинаторики. Парольная политика организации.
Тема 3.2	Основные понятия локальных и глобальных компьютерных сетей. Информационная безопасность в Интернете. Протокол защиты электронной почты S/MIME.	Модель взаимодействия открытых систем ISO/OSI. Основные понятия протокола S/MIME. Структура протокола. Поддержка почтовыми клиентами.
Тема 3.3	Протоколы передачи данных SSL и TLS. Параметры их безопасности.	История разработки протокола. Этапы взаимодействия клиента и сервера. Чем SSL-протокол отличается от SSL-сертификата.
Тема 3.4	Протоколы семейства IPSec: история, архитектура,	Протоколы IPSec и трансляция сетевых адресов. Протоколы AH, ESP, SKIP, ISAKMP, IKE. Типовые

	подключение. Межсетевые экраны и их типы.	схемы подключения межсетевых экранов. Понятие брандмауэра.
Раздел IV	**Анализ и управление рисками в сфере информационной безопасности**	
Тема 4.1	Введение в проблему. Управление рисками.	Понятие риска в сфере информационной безопасности. Исследование рисков. Модель безопасности с полным перекрытием.
Тема 4.2	Методики построения систем защиты информации.	Управление информационной безопасностью. Стандарты ISO/IEC 17799/27002 и 27001. ГОСТ Р ИСО/МЭК 17799:2005. ГОСТ Р ИСО/МЭК 27001-2006.
Тема 4.3	Методики и программные продукты для оценки рисков.	Модель Lifecycle Security. Модель многоуровневой защиты. Методика управления рисками, предлагаемая «Микрософт».

3.4. Организация самостоятельной работы обучающихся

Самостоятельная работа студента – обязательная часть образовательного процесса, направленная на развитие готовности к профессиональному и личностному самообразованию, на проектирование дальнейшего образовательного маршрута и профессиональной карьеры.

Самостоятельная работа обучающихся по дисциплине организована как совокупность аудиторных и внеаудиторных занятий и работ, обеспечивающих успешное освоение дисциплины.

Аудиторная самостоятельная работа обучающихся по дисциплине выполняется на учебных занятиях под руководством преподавателя и по его заданию. Аудиторная самостоятельная работа обучающихся входит в общий объем времени, отведенного учебным планом на аудиторную работу, и регламентируется расписанием учебных занятий.

Внеаудиторная самостоятельная работа обучающихся – планируемая учебная, научно-исследовательская, практическая работа обучающихся, выполняемая во внеаудиторное время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия, расписанием учебных занятий не регламентируется.

Внеаудиторная самостоятельная работа обучающихся включает в себя:

– подготовку к лекциям, зачету;

– изучение учебных пособий;

– изучение теоретического и практического материала по рекомендованным источникам;

– подготовка к защите лабораторных работ;

– подготовка к проверочному тестированию.

Самостоятельная работа обучающихся с участием преподавателя в форме иной контактной работы предусматривает групповую и (или) индивидуальную работу с обучающимися и включает в себя:

– проведение индивидуальных и групповых консультаций по отдельным темам/разделам дисциплины;

– проведение консультаций перед зачетом;

– консультации по организации самостоятельного изучения отдельных разделов/тем.

Перечень разделов/тем/, полностью или частично отнесенных на самостоятельное изучение с последующим контролем:

№ пп	**Наименование раздела /темы дисциплины, выносимые на самостоятельное изучение**	**Задания для самостоятельной работы**	**Виды и формы контрольных мероприятий (учитываются при проведении текущего контроля)**	**Трудоемкость, час**
Раздел IV	**Анализ и управление рисками в сфере информационной безопасности**			

Тема 4.4	Задачи на тему: теоретико-числовые методы в криптографии.	Алгоритм «Аффинный шифр». Алгоритм «Решето Эратосфена».	Разработка программы на языках высокого уровня.	2

3.5. Применение электронного обучения, дистанционных образовательных технологий

Реализация программы учебной дисциплины с применением электронного обучения и дистанционных образовательных технологий регламентируется действующими локальными актами университета.

Учебная деятельность частично проводится на онлайн-платформе за счет применения учебно-методических электронных образовательных ресурсов:

использование ЭО и ДОТ	**использование ЭО и ДОТ**	**объем, час**	**включение в учебный процесс**
обучение с веб-поддержкой	учебно-методические электронные образовательные ресурсы университета 1 категории		организация самостоятельной работы обучающихся
	учебно-методические электронные образовательные ресурсы университета 2 категории		в соответствии с расписанием текущей/промежуточной аттестации

ЭОР обеспечивают в соответствии с программой дисциплины (модуля):

– организацию самостоятельной работы обучающегося, включая контроль знаний обучающегося (самоконтроль, текущий контроль знаний и промежуточную аттестацию),

– методическое сопровождение и дополнительную информационную поддержку электронного обучения (дополнительные учебные и информационно-справочные материалы).

Текущая и промежуточная аттестации по онлайн-курсу проводятся в соответствии с графиком учебного процесса и расписанием.

4. РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, КРИТЕРИИ ОЦЕНКИ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ, СИСТЕМА И ШКАЛА ОЦЕНИВАНИЯ

4.1. Соотнесение планируемых результатов обучения с уровнями сформированности компетенции(й).

Уровни сформированности компетенции(-й)	**Итоговое количество баллов в 100-балльной системе по результатам текущей и промежуточной аттестации**	**Оценка в пятибалльной системе по результатам текущей и промежуточной аттестации**	**Показатели уровня сформированности**		
			универсальной(-ых) компетенции(-й)	**общепрофессиональной(-ых) компетенций**	**профессиональной(-ых) компетенции(-й)**
				ОПК-3: ИД-ОПК-3.1 ИД-ОПК-3.3 ИД-ОПК-3.4 ОПК-4: ИД-ОПК-4.2 ИД-ОПК-4.3	
высокий		отлично/ зачтено (отлично)/ зачтено		Обучающийся: – исчерпывающе и логически стройно излагает учебный материал, применяет знания законов и методов в области естественных и инженерных наук для постановки задачи разработки подсистемы информационной безопасности; – показывает способности в понимании и практическом использовании общенаучных и конкретно-научных методов и принципов исследования; – свободно ориентируется в применении современных информационных технологий и программ для разработки	

				документации: MS Office, SMath Solver и др.*;* – дает развернутые, исчерпывающие, профессионально грамотные ответы на вопросы, в том числе, дополнительные.	
повышенный		хорошо/ зачтено (хорошо)/ зачтено		Обучающийся: – достаточно подробно, грамотно и по существу излагает изученный материал, приводит и раскрывает в тезисной форме основные понятия; – допускает единичные негрубые ошибки; – достаточно хорошо ориентируется в учебной и профессиональной литературе; – ответ отражает знание теоретического и практического материала, не допуская существенных неточностей.	
базовый		удовлетворительно/ зачтено (удовлетворительно)/ зачтено		Обучающийся: – демонстрирует теоретические знания основного учебного материала дисциплины в объеме, необходимом для дальнейшего освоения ОПОП; – демонстрирует фрагментарные знания	

				основной учебной литературы по дисциплине; – ответ отражает знания на базовом уровне теоретического и практического материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профилю обучения.	
низкий		неудовлетворительно/ не зачтено	Обучающийся: – демонстрирует фрагментарные знания теоретического и практического материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации; – испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами; – выполняет задания только по образцу и под руководством преподавателя; – ответ отражает отсутствие знаний на базовом уровне теоретического и практического материала в объеме, необходимом для дальнейшей учебы.		

5. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ, ВКЛЮЧАЯ САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ

5.1. Формы текущего контроля успеваемости, примеры типовых заданий:

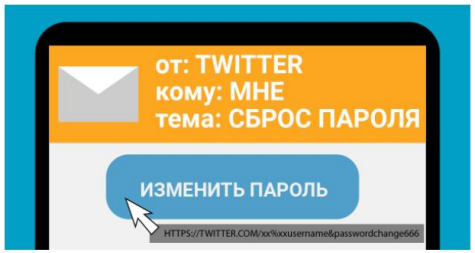
№ пп	Формы текущего контроля	Примеры типовых заданий
1	Выполнение практических работ по разделу I	Практическое занятие 1.1 Использование цифровых сертификатов. Ознакомление с порядком использования цифровых сертификатов X.509 в протоколах защиты данных SSL/TLS и S/MIME. Практическое занятие 1.2 1. Представить число a по основанию системы счисления b, если 1) a = 15321, b = 4; 2) a = 18742, b = 7; 3) $a = (123)_5$, b = 10;

№ пп	Формы текущего контроля	Примеры типовых заданий
		4) $a = (21012)_3$, $b = 10$; 2. Решить задачи • Выяснить, какие из чисел 1589, 1573, 1571, 1591 являются простыми; • Выяснить, какие из чисел 2561, 2669, 2677 являются простыми; • Найти наименьшее натуральное число, которое делится на • 2, 3, 4, 5, 6, 7, 8, 9, 10. • Найти каноническое представление следующих чисел: • 12!; 2) 15!; 3) 18!; 4) 14!; 5) 16!; 6) 17!.
2	Выполнение практических работ по разделу II	Практическое занятие № 2.1 Шифрование данных с применением шифров Цезаря и Атбаш в программе SMath Solver. Примеры типовых заданий: *Задание 1*. Составить программу на языке SMath Solver и зашифровать свою фамилию, записанную заглавными латинскими буквами, с помощью шифра Атбаш. *Задание 2*. Составить программу и зашифровать свою фамилию, записанную заглавными латинскими буквами, с помощью шифра Цезаря. Методы перестановки Примеры типовых заданий: *Задание 3*. Зашифруйте методом перестановки с фиксированным периодом d=6 с ключом 436215 сообщения: ○ ЖЕЛТЫЙ_ОГОНЬ ○ МЫ_НАСТУПАЕМ *Задание 4*. Расшифруйте сообщения, зашифрованные методом перестановки с фиксированным периодом d=8 с ключом 64275813: ○ СЛПИЬНАЕ ○ РОИАГДВН *Задание 5*. Определите ключи в системе шифрования, использующей перестановку с фиксированным периодом d=5 по парам открытых и зашифрованных сообщений: ○ МОЙ ПАРОЛЬ – ЙПМ ООЬАЛР ○ СИГНАЛ БОЯ – НИСАГО ЛЯБ

№ пп	Формы текущего контроля	Примеры типовых заданий
		Задание 6. Зашифруйте сообщения методом перестановки по таблице 5*5. Ключ указывает порядок считывания столбцов при шифровании. o ШИРОКОПОЛОСНЫЙ УСИЛИТЕЛЬ (ключ: 41235) o ПЕРЕДАЧА ИЗОБРАЖЕНИЯ (ключ: 24513)
		Практическое занятие № 2.2 Шифрование данных. Реализация таблицы Вижинера средствами Ms EXCEL. Примеры типовых заданий: *Задание 1*. Пусть исходный алфавит содержит следующие символы: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ Зашифруйте с помощью шифра Вижинера и ключа ЯБЛОКО сообщения: o КРИПТОСТОЙКОСТЬ o ГАММИРОВАНИЕ *Задание 2*. Пусть исходный алфавит состоит из следующих знаков (символ «_» (подчеркивание) будем использовать для пробела): АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ_ Расшифруйте сообщения, зашифрованные с помощью шифра Вижинера и ключа ОРЕХ: o ШВМБУЖНЯ o ЯБХЪШЮМХ
		Практическое занятие № 2.3 1. Сгенерируйте открытый и закрытый ключи в алгоритме шифрования RSA, выбрав простые числа p и q из первой сотни. Зашифруйте и расшифруйте сообщение, состоящее из ваших инициалов: ФИО. 2. Пусть e, d – соответственно секретный и открытый ключи абонента A; p, q – простые числа абонента A; m – передаваемое сообщение абоненту A. Найти d и шифрованное сообщение y, передаваемое абоненту A, если известно, что: 1) p=5, q=11, e=3, m=8 2) p=5, q=11, e=7, m=3 3. Шифр Эль-Гамаля. Пусть x, y – соответственно секретный и открытый ключи абонента A, p – простое число, g – первообразный корень по модулю p (параметры шифрсистемы), m – передаваемое сообщение абоненту A, k – случайное число. Найти y и шифрованное сообщение (c1, c2), передаваемое абоненту A, если известно, что: 1) p=13, q=2, x=5, k=3, m=10

№ пп	Формы текущего контроля	Примеры типовых заданий
		2) p=13, q=2, x=6, k=3, m=3
		Практическое занятие № 2.4 *Задание 1*. Подпись Эль-Гамаля. Пусть p – простое число, g – первообразный корень по модулю p, x y – соответственно секретный и открытый ключи абонента A, M – подписываемое сообщение, k – случайное число. Найти y, подписать сообщение M подписью абонента A и проверить подпись, если известно, что: 1) p = 11, g =2, x = 5, k = 3, M = 21; 2) p = 13, g =2, x = 8, k = 11, M = 20. *Задание 2*. Подпись Шнорра. Пусть p – простое число, q – простой делитель числа p – 1, g – элемент из кольца вычетов по модулю p, x y – соответственно секретный и открытый ключи абонента A, M – подписываемое сообщение, k – случайное число. Найти y, подписать сообщение M подписью абонента A и проверить подпись, если известно, что: 1) p = 13, q = 3, g = 3, x = 2, k = 2, M = 11; 2) p = 11, q = 5, g = 9, x = 4, k = 3, M = 21;
5	Выполнение практических работ по разделу III	Практическое занятие № 3.1 Управление доступом в СУБД SQL Server.
6		Практическое занятие № 3.2 Создание центра сертификации (удостоверяющего центра) в Windows Server 2008. Приобретение практических навыков развертывания и настройки центра сертификации встроенными средствами Windows Server 2008.
7		Практическое занятие № 3.3 Встроенный межсетевой экран Windows Server 2008. Приобретение практических навыков настройки межсетевого экрана Использование Microsoft Security Assessment Tool.
8	Выполнение практических работ по разделу IV	Практическое занятие № 4.1 Установка Avast Free Antivirus. Развертывание антивирусной защиты: установка агентов администрирования, проверка совместимости.
9		Практическое занятие № 4.2 Работа с вирусными инцидентами.
10		Практическое занятие № 4.3 Приобретение практических навыков настройки разрешений на доступ к объектам баз данных в среде СУБД Ms SQL Serve 2008/2021. Настройка протокола IPSec в Windows Server.

№ пп	Формы текущего контроля	Примеры типовых заданий
11	Контрольное тестирование по разделу I «Теоретические основы информационной безопасности»	Примеры тестовых вопросов: 1. Что такое шифрование? А) способ изменения документа или другого сообщения, обеспечивающее искажение его содержимого Б) преобразование текста в код В) упорядоченный набор из элементов алфавита 2. Пространство ключей k – это… А) набор возможных значений ключа Б) длина ключа В) нет правильного ответа
12	Контрольное тестирование по разделу II «Основы криптографии»	Примеры тестовых вопросов: 1. Что такое криптография? А) наука, изучающая структуру, общие свойства и методы передачи информации, в том числе связанной с применением ЭВМ Б) наука о математических методах обеспечения конфиденциальности и аутентичности информации В) процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов 2. Символы исходного текста складываются с символами некой случайной последовательности – это… А) алгоритм гаммирования Б) алгоритм перестановки В) алгоритм замены
13	Контрольное тестирование по разделу III «Защита информации в IP-сетях»	Примеры тестовых вопросов: 1. Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей: A) Пустые письма B) Черный пиар C) Фишинг D) Вирус 2. Когда применяются алгоритмы шифрования информации A) Когда мы не доверяем месту, где храним информацию B) Когда нам требуется подтверждения подлинности отправителя C) Когда мы не доверяем каналам связи, по которым передаем информацию D) Во всех перечисленных случаях

№ пп	Формы текущего контроля	Примеры типовых заданий
14	Контрольное тестирование по разделу III «Анализ и управление рисками в сфере информационной безопасности»	Примеры тестовых вопросов: 1. Что не относится к сведениям конфиденциального характера? A) Персональные данные B) Сведения, составляющие тайну следствия C) Сведения о сущности изобретения D) Сведения о задолженности работодателей по выплате заработной платы и социальным выплатам **2.** Вы забыли свой пароль от Twitter и решили его сбросить. Вскоре вам приходит письмо. Оно кажется подозрительным. Или нет?  А) Нет. Б) Да.

5.2. Критерии, шкалы оценивания текущего контроля успеваемости:

Наименование оценочного средства (контрольно-оценочного мероприятия)	Критерии оценивания	Шкалы оценивания	
		100-балльная система	Пятибалльная система
Практическое задание	Задание выполнено полностью. Нет ошибок в логических рассуждениях. Возможно наличие одной неточности или описки, не являющиеся следствием незнания или непонимания учебного материала. Обучающийся показал полный объем знаний, умений в освоении, пройденных тем и применение их на практике.		5
	Задание выполнено полностью, но обоснований шагов решения недостаточно. Допущена одна ошибка или два-три недочета.		4

Наименование оценочного средства (контрольно-оценочного мероприятия)	Критерии оценивания	Шкалы оценивания		
		100-балльная система	Пятибалльная система	
	Допущены более одной ошибки или более двух-трех недочетов.		3	
	Задание выполнено не полностью. Допущены грубые ошибки.		2	
	Задание не выполнено.			
Тест	За выполнение каждого тестового задания испытуемому выставляются баллы. Номинальная шкала предполагает, что за правильный ответ к каждому заданию выставляется один балл, за не правильный — ноль. В заданиях с выбором нескольких верных ответов, заданиях на установление правильной последовательности, заданиях на установление соответствия, заданиях открытой формы используют порядковую шкалу. В этом случае баллы выставляются не за всё задание, а за тот или иной выбор в каждом задании, например, выбор варианта, выбор соответствия, выбор ранга, выбор дополнения.		5	85% - 100%
			4	65% - 84%
			3	41% - 64%
			2	40% и менее 40%

5.3. Система оценивания результатов текущего контроля и промежуточной аттестации.

Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.

Форма контроля	100-балльная система	Пятибалльная система
Текущий контроль:		
- практические задания		2 – 5 или зачтено/не зачтено
- проверочные тесты		2 – 5 или зачтено/не зачтено
Промежуточная аттестация: зачет по совокупности результатов текущего контроля успеваемости		отлично хорошо удовлетворительно неудовлетворительно зачтено не зачтено
Итого за семестр (дисциплину) зачёт/зачёт с оценкой/экзамен		

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Реализация программы предусматривает использование в процессе обучения следующих образовательных технологий:

- групповых дискуссий;
- проблемная лекция;
- анализ ситуаций и имитационных моделей;
- поиск и обработка информации с использованием сети Интернет;
- дистанционные образовательные технологии: платформа Moodle, сервисы Goggle-meet, Zoom;
- применение электронного обучения: применение инструментов MS Office (Word, Excel, Power Point);
- использование на лекционных занятиях видеоматериалов и наглядных пособий;
- самостоятельная работа в системе компьютерного тестирования.

7. ПРАКТИЧЕСКАЯ ПОДГОТОВКА

Практическая подготовка в рамках учебной дисциплины не реализуется.

8. ОРГАНИЗАЦИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

При обучении лиц с ограниченными возможностями здоровья и инвалидов используются подходы, способствующие созданию безбарьерной образовательной среды: технологии дифференциации и индивидуального обучения, применение соответствующих методик по работе с инвалидами, использование средств дистанционного общения, проведение дополнительных индивидуальных консультаций по изучаемым теоретическим вопросам и практическим занятиям, оказание помощи при подготовке к промежуточной аттестации.

При необходимости рабочая программа дисциплины может быть адаптирована для обеспечения образовательного процесса лицам с ограниченными возможностями здоровья, в том числе для дистанционного обучения.

Учебные и контрольно-измерительные материалы представляются в формах, доступных для изучения студентами с особыми образовательными потребностями с учетом нозологических групп инвалидов:

Для подготовки к ответу на практическом занятии, студентам с ограниченными возможностями здоровья среднее время увеличивается по сравнению со средним временем подготовки обычного студента.

Для студентов с инвалидностью или с ограниченными возможностями здоровья форма проведения текущей и промежуточной аттестации устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.).

Промежуточная аттестация по дисциплине может проводиться в несколько этапов в форме рубежного контроля по завершению изучения отдельных тем дисциплины. При необходимости студенту предоставляется дополнительное время для подготовки ответа на зачете или экзамене.

Для осуществления процедур текущего контроля успеваемости и промежуточной аттестации обучающихся создаются, при необходимости, фонды оценочных средств, адаптированные для лиц с ограниченными возможностями здоровья и позволяющие оценить достижение ими запланированных в основной образовательной программе результатов обучения и уровень сформированности всех компетенций, заявленных в образовательной программе.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Характеристика материально-технического обеспечения дисциплины составляется в соответствии с требованиями ФГОС ВО.

Материально-техническое обеспечение дисциплины при обучении с использованием традиционных технологий обучения.

Наименование учебных аудиторий, лабораторий, мастерских, библиотек, спортзалов, помещений для хранения и профилактического обслуживания учебного оборудования и т.п.	**Оснащенность учебных аудиторий, лабораторий, мастерских, библиотек, спортивных залов, помещений для хранения и профилактического обслуживания учебного оборудования и т.п.**
119071, г. Москва, Малый Калужский переулок, дом 1	
аудитории для проведения занятий лекционного типа	комплект учебной мебели; технические средства обучения, служащие для представления учебной информации аудитории: – ноутбук; – проектор
аудитории для проведения лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	комплект учебной мебели; технические средства обучения, служащие для представления учебной информации аудитории: – ноутбук, – проектор; 12 персональных компьютеров.
Помещения для самостоятельной работы обучающихся	**Оснащенность помещений для самостоятельной работы обучающихся**
читальный зал библиотеки:	компьютерная техника; подключение к сети «Интернет»
аудитории для проведения лабораторных занятий	комплект учебной мебели; 12 персональных компьютеров.

Материально-техническое обеспечение учебной дисциплины при обучении с использованием электронного обучения и дистанционных образовательных технологий.

Необходимое оборудование	**Параметры**	**Технические требования**

Персональный компьютер/ ноутбук/планшет, камера, микрофон, динамики, доступ в сеть Интернет	Веб-браузер	Версия программного обеспечения не ниже: Chrome 72, Opera 59, Firefox 66, Edge 79, Яндекс.Браузер 19.3
	Операционная система	Версия программного обеспечения не ниже: Windows 7, macOS 10.12 «Sierra», Linux
	Веб-камера	640x480, 15 кадров/с
	Микрофон	любой
	Динамики (колонки или наушники)	любые
	Сеть (интернет)	Постоянная скорость не менее 192 кБит/с

Технологическое обеспечение реализации программы осуществляется с использованием элементов электронной информационно-образовательной среды университета Moodle.

10. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ/УЧЕБНОГО МОДУЛЯ

№ п/п	Автор(ы)	Наименование издания	Вид издания (учебник, УП, МП и др.)	Издательство	Год издания	Адрес сайта ЭБС или электронного ресурса *(заполняется для изданий в электронном виде)*	Количество экземпляров в библиотеке Университета
10.1 Основная литература, в том числе электронные издания							
1	Нестеров С. А.	Основы информационной безопасности	Учебник	Издательство ЛАНЬ	2021	https://znanium.com/catalog/document?id=379717	
2	Гришина Н.В.	Основы информационной безопасности	Учебное пособие	М.: НИЦ ИНФРА-М	2021	https://znanium.com/catalog/document?id=379717	
3	Рацеев С.М.	Математические методы защиты информации и их основы	Учебное пособие	Издательство ЛАНЬ	2023	https://znanium.com/catalog/document?id=379717	
10.2 Дополнительная литература, в том числе электронные издания							
4	Новиков В.К.	Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации)	Учебное пособие	Издательство: Горячая линия-Телеком	2015	https://znanium.com/catalog/document?id=67242	5
10.3 Методические материалы (указания, рекомендации по освоению дисциплины (модуля) авторов РГУ им. А. Н. Косыгина)							
5	Бойцев О.М.	Защити свой компьютер на 100 % от вирусов и хакеров	Практическое пособие	Издательство: Питер	2008	https://znanium.com/catalog/document?id=379882	5

11. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА

11.1. Ресурсы электронной библиотеки, информационно-справочные системы и профессиональные базы данных:

№ пп	Электронные учебные издания, электронные образовательные ресурсы
1.	ЭБС «Лань» http://www.e.lanbook.com/
2.	«Znanium.com» научно-издательского центра «Инфра-М» http://znanium.com/
3.	Электронные издания «РГУ им. А.Н. Косыгина» на платформе ЭБС «Znanium.com» http://znanium.com/
4.	Электронные ресурсы компании ЦИТМ Экспонента https://exponenta.ru/
	Профессиональные базы данных, информационные справочные системы
1.	Энциклопедия АСУ ТП. https://www.bookasutp.ru/
2.	Всероссийская патентно-техническая библиотека https://www1.fips.ru/about/vptb-otdelenie-vserossiyskaya-patentno-tekhnicheskaya-biblioteka/index.php
3.	Наукометрическая база данных Scopus https://www.scopus.com/home.uri
4.	Наукометрическая база данных Web of Science https://access.clarivate.com/
5.	Российская государственная библиотека https://www.rsl.ru/
6.	Поисковая система PatSearch
7.	Национальная электронная библиотека (НЭБ)

11.2. Перечень программного обеспечения

№п/п	Программное обеспечение	Реквизиты подтверждающего документа/ Свободно распространяемое
1.	Windows 10 Pro, MS Office 2019	контракт № 18-ЭА-44-19 от 20.05.2019
2.	PrototypingSketchUp: 3D modeling for everyone	контракт № 18-ЭА-44-19 от 20.05.2019
3.	Программное обеспечение Matlab R2019a	контракт № 18-ЭА-44-19 от 20.05.2019
4.	Программное обеспечение Mathcad Prime 6.0	контракт № 18-ЭА-44-19 от 20.05.2019

ЛИСТ УЧЕТА ОБНОВЛЕНИЙ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ/МОДУЛЯ

В рабочую программу учебной дисциплины/модуля внесены изменения/обновления и утверждены на заседании кафедры:

№ пп	год обновления РПД	характер изменений/обновлений с указанием раздела	номер протокола и дата заседания кафедры