МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И
МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

Утверждаю
Зам. директора по УВР
_____ А.Г. Жуковский
«_21_» ___08_____ 2022 г.

Криптографические протоколы Б1.О.35
рабочая программа дисциплины

Кафедра: Инфокоммуникационные технологии и системы связи
Направление подготовки: **10.03.01 Информационная безопасность**
Профиль: **Безопасность компьютерных систем.**
Формы обучения: **очная**

Распределение часов дисциплины по семестрам (для очной формы обучения), курсам (для заочной формы обучения)

Вид учебной работы	ОФ		ЗФ	
	ЗЕ	часов	ЗЕ	часов
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	4	144/7сем		
Контактная работа, в том числе (по семестрам, курсам):		72/7сем		
Лекции		34/7сем		
Лабораторных работ				
Практических занятий		38/7 сем		
Семинаров				
Самостоятельная работа		36/7 сем		
Контроль		36		
Число контрольных работ (по курсам)				
Число КР (по семестрам, курсам)				
Число КП (по семестрам, курсам)				
Число зачетов с оценкой с разбивкой по семестрам (курсам)				
Число экзаменов с разбивкой по семестрам (курсам)		1/7сем		

Программу составил:
Доцент кафедры ИТСС, к.т.н., доцент Шухардин А.Н.

Рецензент:
Ведущий сотрудник ФГУП «РНИИРС», д.т.н., доцент Елисеев А.В.

Рабочая программа дисциплины
«Криптографические протоколы»

разработана в соответствии с ФГОС ВО:
направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства образования и науки Российской Федерации от 17 ноября 2020г. N 1427.

Составлена на основании учебного плана
направления 10.03.01 «Информационная безопасность», профиля «Безопасность компьютерных систем», одобренного Учёным советом СКФ МТУСИ, протокол № 9 от 25.04.2022 г., и утвержденного директором СКФ МТУСИ 25.04.2022 г.

Рассмотрена и одобрена на заседании кафедры
«Инфокоммуникационные технологии и системы связи»

Протокол от «29» 08 2022 г. № 1

Зав. кафедрой _____ В.И. Юхнов

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР ________________
«___» _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры

«Инфокоммуникационные технологии и системы связи»

Протокол от «___» _______ 20__ г. № ____
Зав. кафедрой _____________________

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР ________________
«___» _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
«Инфокоммуникационные технологии и системы связи»

Протокол от «___» _______ 20__ г. № ____
Зав. кафедрой _____________________

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР ________________
«___» _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
«Инфокоммуникационные технологии и системы связи»

Протокол от «___» _______ 20__ г. № ____
Зав. кафедрой _____________________

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР ________________
«___» _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
«Инфокоммуникационные технологии и системы связи»

Протокол от «___» _______ 20__ г. № ____
Зав. кафедрой _____________________

1. Цели изучения дисциплины

Целью освоения дисциплины является формирование у обучаемых знаний в области существующих подходов к анализу и синтезу криптографических протоколов, с государственными и международными стандартами в этой области.

Задачи освоения дисциплины:

- формирование знаний, умений и навыков, позволяющих анализировать, создавать и использовать криптографические протоколы для защиты информации,
- освоение принципов корректного применения современных защищенных информационных технологий.

2. Планируемые результаты обучения

Изучение дисциплины направлено на формирование у выпускника способности решать профессиональные задачи в соответствии с ***эксплуатационным*** видом деятельности:

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

Компетенции выпускника, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)
ОПК-8: Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности
ОПК-9: Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности
Знать:
- национальные стандарты Российской Федерации в области криптографической защиты информации и сферы их применения; - основные математические методы и алгоритмы шифрования, расшифрования и дешифрования сообщений; - виды криптографических протоколов и их место в комплексной системе защиты информации; - основные виды средств криптографической защиты информации (СКЗИ), включая блочные и поточные системы шифрования, криптографические системы с открытым ключом, криптографические хеш- функции и криптографические протоколы; - принципы функционирования программных средств криптографической защиты информации; - алгоритмы электронной (цифровой) подписи в телекоммуникационных системах.
Уметь:
- анализировать угрозы безопасности информации в компьютерных сетях; - использовать криптографические протоколы, применяемые в компьютерных сетях.
Владеть:
- навыками анализа и оценки угроз информационной безопасности объекта информатизации; - навыками установки программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации.

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Дисциплина «Криптографические протоколы» включена в обязательную часть (блок

	Б1.О) учебного плана по направлению «Информационная безопасность». Ей предшествует изучение дисциплины «Основы информационной безопасности», «Методы и средства криптографической защиты информации».
2	Успешное освоение дисциплины «Криптографические протоколы» базируется также на знаниях, приобретенных из дисциплин: Б1.О.03 «Информатика», Б1.О.05 «Математический анализ», Б1.О.13 «Теория вероятности и математическая статистика».
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Дисциплина является необходима для успешного освоения дисциплин: Б1.О.39 «Методы оценки безопасности компьютерных систем (Аудит компьютерных систем)», Б1.О.40 «Администрирование средств защиты информации в компьютерных системах и сетях».

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 144 часов, 72 аудиторных часов, 36 часов самостоятельной работы, 36 часов контроль)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
Курс 4, Семестр 7					
Модуль 1. Криптографические протоколы и их классификация (36+18) часов					
1.1	Лекция №1. КРИПТОГРАФИЧЕСКОГО ПРОТОКОЛЫ. Роль криптографических протоколов в системах защиты информации. Свойства протоколов, характеризующие их безопасность. Основные виды уязвимостей. Подходы к классификации криптографических протоколов. Подходы к моделированию криптографических протоколов	Л1	2	ОПК-8 ОПК-9	Л1.1 Л1.2
1.2	Лекция №2. Понятие уязвимости и атаки на криптографический протокол. Основные виды криптографических систем.	Л2	2	ОПК-8 ОПК-9	Л1.1 Л1.2
1.3	Практическое занятие № 1 Использование симметричных и асимметричных шифрсистем для построения криптографических протоколов. Примеры. Основные подходы к автоматизации анализа протоколов.	ПЗ1	4	ОПК-8 ОПК-9	Л3.1
1.4	Лекция №3. КРИПТОГРАФИЧЕСКИЕ ХЕШ-ФУНКЦИИ. Хэш-функции MD-5, семейство SHA	Л3	2	ОПК-8 ОПК-9	Л1.1 Л1.2
1.5	Практическое занятие № 2 Функции хеширования: ГОСТ Р34.11-94, MD5, SHA	ПЗ2	4	ОПК-8 ОПК-9	Л3.1
1.6	Лекция № 4 СХЕМЫ ЦИФРОВОЙ ПОДПИСИ. Схемы цифровой подписи на основе симметричных и асимметричных шифрсистем. Схемы Эль-Гамаля, Нюберг-Рюппеля и Шнорра, их	Л4	2	ОПК-9	Л1.1 Л1.2

	свойства Семейство схем типа ЭльГамаля.				
1.7	Лекция № 5 Одноразовые подписи. Схемы конфиденциальной цифровой подписи и подписи вслепую. Подписи с обнаружением подделки.	Л5	2	ОПК-9	Л1.1 Л1.2
1.8	Практическое занятие №3 Стандарты США и России электронной цифровой подписи.	ПЗ3	4	ОПК-8 ОПК-9	Л3.1
198	Лекция №6 ПРОТОКОЛЫ ГЕНЕРАЦИИ И ПЕРЕДАЧИ КЛЮЧЕЙ Протоколы на основе симметричных и асимметричных шифрсистем. Двух и трех сторонние протоколы передачи и распределения ключей. Функции доверенной третьей стороны и выполняемые ею роли.	Л6	2	ОПК-9	Л1.1 Л1.2
1.9	Лекция № 7. СХЕМЫ ПРЕДВАРИТЕЛЬНОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ. Протокол открытого распределения ключей Диффи-Хеллмана и способы его защиты от атаки «противник в середине». Аутентифицированные протоколы открытого распределения ключей.	Л7	2	ОПК-9	Л1.1 Л1.2
1.8	Практическое занятие № 4 Протокол открытого распределения ключей Диффи-Хеллмана.	ПЗ4	4	ОПК-9	Л3.1
1.9	Лекция № 8. Групповые протоколы. Протоколы разделения секрета и распределения ключей для телеконференции.	Л8	2	ОПК-9	Л1.1 Л1.2
1.10	Практическое занятие № 5 Групповые протоколы. Протоколы разделения секрета и распределения ключей для телеконференции	ПЗ5	4	ОПК-9	Л3.1
1.11	Федеральный закон Российской Федерации «Об электронной подписи» 6.04.2011г. № 63-ФЗ РФ Нормативно-правовые акты Российской Федерации о ведении электронного документооборота.	СРС	18	ОПК-8 ОПК-9	Л1.1 Л1.2
Модуль 2 Прикладные криптографические протоколы (36+18)					
2.1	Лекция №9. Протоколы идентификации. Протоколы идентификации на основе паролей, протоколы “рукопожатия” и типа «запрос-ответ»..	Л9	2	ОПК-8 ОПК-9	Л1.1 Л1.2
2.2	Лекция № 10. Идентификация с использованием систем открытого шифрования. Понятие протоколов интерактивного доказательства и доказательства знания. Протоколы Фиата-Шамира, Шаума, Шнорра и Окамото.	Л10	2	ОПК -9	Л1.1 Л1.2
2.3	Лекция № 11. Связь между протоколами цифровой подписи и	Л11	2	ОПК-8 ОПК-9	Л1.1 Л1.2

	протоколами идентификации. Протоколы с самосертифицируемыми открытыми ключами, построенными на основе идентификаторов.				
2.4	Практическое занятие № 6 Протоколы идентификации.	ПЗ6	4	ОПК-9	Л3.1
2.5	Лекция № 12. Протоколы с нулевым разглашением Протоколы решения математических задач. Протокол привязки к биту. Игровые протоколы. Подбрасывание монеты по телефону. Протоколы подписания контрактов.	Л12	2	ОПК-8 ОПК-9	Л1.1 Л1.2
2.6	Лекция № 13. Сертифицированная электронная почта. Аргумент с нулевым разглашением. Схемы электронного голосования.	Л13	2	ОПК-8 ОПК-9	Л1.1 Л1.2
2.7	Практическое занятие №7 Протоколы решения математических задач.	ПЗ7	4	ОПК-9	Л3.1
2.8	Лекция № 14. Базовый протокол с нулевым разглашением (Жан-Жак Кискате (Jean-Jfcques Quisquater) и Луи Гилу (Louis Guillou)).	Л14	2	ОПК-8 ОПК-9	
2.9	Практическое занятие № 8 Схемы электронного голосования	ПЗ8	2	ОПК-8 ОПК-9	Л3.1
2.10	Лекция № 15. Особенности построения семейства протоколов IPsec	Л15	2	ОПК-8 ОПК-9	Л1.1 Л1.2
2.11	Лекция № 16. Протоколы SSL/TLS и особенности их реализации.	Л16	2	ОПК-8 ОПК-9	Л1.1 Л1.2
2.12	Практическое занятие № 9 Особенности построения семейства протоколов IPsec. Протоколы SSL/TLS и особенности их реализации.	ПЗ9	4	ОПК-8 ОПК-9	Л3.1
2.13	Лекция № 17. Электронные платежи и электронные монеты. Криптовалюты и блокчейн	Л17	2	ОПК-8 ОПК-9	Л1.1 Л1.2
2.14	Практическое занятие № 10 Криптовалюты.	ПЗ 10	4	ОПК-8 ОПК-9	Л3.1
2.16	Анализ моделей нарушителя; угрозы информационно-программному обеспечению вычислительных систем и их классификация. Использование криптографических методов для защиты данных, циркулирующих в вычислительной сети.	СРС	18	ОПК-8 ОПК-9	Л1.1 Л1.2
Экзамен – 36 часов					
Итого – 144 часа					

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Рекомендуемая литература				
5.1.1. Основная литература				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л1.1	Лапонина О. Р.	Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : учебное пособие / О. Р. Лапонина ; под редакцией В. А. Сухомлина. — 3-е изд. https://www.iprbookshop.ru/97571.html	М. : ИНТУИТ, Ай Пи Ар Медиа, 2020. — 605 с.	Э1
Л1.2	Баранова Е.К., Бабаш А.В.	Информационная безопасность и защита информации : учеб. пособие / — 3-е изд., перераб. и доп.	М. : РИОР : ИНФРА-М, 2017. — 322 с.	Э2
6.1.2. Дополнительная литература				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л2.1	Косолапов Ю. В.	Криптографические протоколы на основе линейных кодов : учебное пособие / Ю. В. Косолапов. https://www.iprbookshop .ru/100176 .html	Ростов-на-Дону, Таганрог : Изд-во ЮФУ, 2020. — 98 с.	Э3
Л2.2	Лось А.Б.	Криптографические методы защиты информации. Учебник для академического бакалавриата / А.Б. Лось, А.Ю. Нестеренко. М.И. Рожков - Режим доступа: http://znanium.com/catalog/product/474838	М.: Изд-во Юрайт, 2016.-476 с	Э4
6.1.3. Учебно-методическое обеспечение для самостоятельной работы обучающихся				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л3.1	Шевчук П.С.	Методические указания по проведению практических занятий по дисциплине «Криптографические протоколы» / П.С. Шевчук. – Ростов-на -Дону: Изд-во СКФ МТУСИ, 2015. – 53 с.: ил.	РнД: СКФ МТУСИ, 2016	Э5
6.2. Электронные образовательные ресурсы				
Э1	https://www.iprbookshop.ru/97571 .html			
Э2	http://znanium.com/catalog/product/763644			
Э3	https://www.iprbookshop.ru/100176.html			
Э4	http://znanium.com/catalog/product/474838			
Э5	http://www.skf-mtusi.ru/?page_id=659			
6.3. Программное обеспечение				
П.1	Window 8,10			
П.2	Word processor Microsoft Word or LibreOffice Writer или аналог.			
П.3	MS Power Point или аналог.			

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оборудованная интерактивной доской, проектором
6.2 МТО и практических занятий	

1	Компьютерная аудитория с выходом в интернет
6.3 МТО рубежных контролей, экзамена	
1	Компьютерная аудитория

7. Методические указания для обучающихся по освоению дисциплины

7.1 Указания по самостоятельной работе студента

Достижение целей эффективной подготовки студентов в вузах невозможно без их целеустремленной самостоятельной работы. При этом, безусловно, нельзя обойтись без живого общения и консультирования со стороны профессорско-преподавательского состава Самостоятельная работа студентов является составной частью учебной работы и имеет целью закрепление и углубление полученных знаний и навыков, поиск и приобретение новых знаний, в том числе с использованием автоматизированных обучающих курсов (систем), а также выполнение учебных заданий, подготовку к предстоящим занятиям, зачетам и экзаменам. Обязательным компонентом самостоятельной работы студентов является внеаудиторный практикум по иностранному языку.

Самостоятельная работа организуется преподавателями, обеспечивается и контролируется кафедрами. Она предусматривает, как правило, разработку рефератов, выполнение расчетно-графических, вычислительных работ, моделирования и других творческих заданий в соответствии с учебной программой (тематическим планом изучения дисциплины). Основная цель данного вида занятий состоит в обучении курсантов методам самостоятельной работы с учебным материалом.

Материал, подлежащий обработке на самостоятельных занятиях, намечается при разработке программы самостоятельной работы. Опыт, накопленный кафедрами в организации самостоятельных занятий, что материал, выделяемый на такие занятия, должен удовлетворять следующим требованиям:

- быть изложенным в учебнике достаточно полно и с примерами;
- обеспечиваться достаточным количеством литературы, учебных пособий. учебно-методических материалов, образцов техники
- содержать материал. углубляющий знания, полученные на лекции;
- осваивать проблемные еще не полностью решенные вопросы.

Проведению самостоятельной работы (как и любого другого вида занятий) должна предшествовать подготовка как преподавателя, так и обучаемых.

Постановку задачи обучаемым на проведение самостоятельного занятия преподаватель осуществляет на одном из занятия, предшествующему данному. Он разъясняет смысл занятия и указывает, что к нему студенты должны приготовить. Задание на самостоятельную работу должно быть выдано заблаговременно с тем, чтобы слушатели имели время на информационный поиск в библиотеке необходимых пособий.

Методику самостоятельной работы все обучаемые выбирают индивидуально, но методика достижения конечной цели может определяться преподавателем и включать: последовательность изучения и усвоения учебно-методического материала, пособий, руководств, наставлений, техники и т.д.; определение главного в изучаемом материале, материале, который необходимо законспектировать; просмотр учебных кинофильмов и их обсуждение; работу студентов по индивидуальным заданиям; опрос обучаемых в течении 7-10 минут с целью проверки усвоения главного из прочитанного материала.

При возникновении затруднений у обучаемых в разрешении вопросов задания преподавателю необходимо предусмотреть, чтобы каждый обучаемый мог получить оперативную консультацию по любому вопросу, если же при самостоятельной работе возникают затруднения по одному и тому же материалу (вопросу) у многих обучаемых, то желательно провести групповую консультацию.

Для контроля усвоения учебного материала целесообразно проводить в групповое собеседование или обсуждение изучаемого материала, проведение контрольных работ и т.п. Контрольные мероприятия при должной их организации позволяют не только оценивать знания материала, но и углубить и закрепить его у обучаемых.

Приветствуется использование компьютеров, которое:

- расширяет информационную баз) учебных занятий;
- повышает активность обучаемых, из пассивного получателя информации они превращаются в её добытчиков:
- способствует развитию способностей к анализу и обобщению, улучшает связанность, широту и глубину мышления;
- облегчает усвоение абстрактного материала, позволяет многое из него представить в виде конкретных образов;
- приучает к точности, аккуратности, последовательности действий способствует развитию самостоятельности.

Компьютерные технологии и программные продукты для выполнения самостоятельной работы по освоению учебного материала необходимо использовать в соответствии с указаниями методических разработок раздела 5 настоящей Рабочей программы.

Для более углубленного изучения материала по дисциплине целесообразно использовать учебные курсы сайта http://www.intuit.ru/ .

Таблица 7.1 – Учебный материал, выносимый на самостоятельное изучение студентам очной формы обучения

№	Темы, разделы, вынесенные на самостоятельную подготовку, вопросы для подготовки к практическим и лабораторным занятиям; курсовые работы, содержание контрольных работ; рекомендации по использованию литературы, ЭВМ и др.	Часов всего: 36	Неделя
Модуль 1 – 18 часов			
1	Нормативно-правовые акты Российской Федерации о ведении электронного документооборота.	14	1-6
2	Федеральный закон Российской Федерации «Об электронной подписи» 6.04.2011г. № 63-ФЗ РФ.	4	7-8
Модуль 2 –18 часов			
3	Анализ моделей нарушителя; угрозы информационно-программному обеспечению вычислительных систем и их классификация.	8	9-12
4	Использование криптографических методов для защиты данных, циркулирующих в вычислительной сети	10	13-16

Дополнения и изменения в рабочей программе