Федеральное агентство связи
Колледж телекоммуникаций
ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

УТВЕРЖДЕНО
приказом директора КТ МТУСИ
№ 01-03-1137/1 от «19» июня 2020
_____ С.Н. Ильиных

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.12 ОСНОВЫ КРИПТОГРАФИИ

для специальности
10.02.04 «Основы информационной безопасности телекоммуникационных систем»
(очная форма обучения)

Москва, 2020г.

ОДОБРЕНА
Цикловой (предметной) комиссией
Компьютерных систем и безопасности
наименование комиссии

Протокол № 5
от «09» июня 2020 г.

Председатель цикловой (предметной) комиссии

_____ / Сергеева М.Б/

Разработано на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем (приказ Минобрнауки России № 1551 от 09 декабря 2016 года) и примерной основной образовательной программы 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.
Зарегистрировано в государственном реестре примерных основных образовательных программ под № 10.02.04-170703

Рассмотрено и одобрено на заседании методического совета
«10» июня 2020 г. Протокол № 5

СОГЛАСОВАНА:
Начальник методического отдела

_____ / Л.М.Кузнецова/
Подпись Ф.И.О.

Организация-разработчик:
КТ МТУСИ, Г. Москва

Разработчик:
Преподаватель КТМТУСИ: Сергеева М.Б.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1. Область применения рабочей программы

Рабочая программа учебной дисциплины ОП.12 Основы криптографии является частью образовательной программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

1.2. Место дисциплины в структуре основной профессиональной образовательной программы:

Учебная дисциплина ОП.12 Основы криптографии входит в перечень вариативных учебных дисциплин учебного плана в соответствии с потребностями работодателей и спецификой деятельности образовательной организации, входит в общепрофессиональный цикл.

1.3. Планируемые результаты освоения дисциплины:

Код ПК, ОК	Умения	Знания
ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 09, ОК 10, ПК 2.1, ПК 2.2, ПК 2.3	производить элементарные операции над шифрами - моно- и многоалфавитные подстановки, системы шифрования Виженера, шифр Плейфера перестановки, гаммирование; − работать со стандартами шифрования DES, блочными шифрами; − использовать алгоритм, криптосистемы без передачи ключей; − составлять протоколы аутентификации; − применять цифровую подпись	основные алгоритмы шифрования с секретным и открытым ключом; − криптосистемы на базе алгоритмов Диффи-Хелмана, Эль-Гамаля, RSA, и т.д.; − основные положения криптографических протоколов аутентификации и «электронной подписи».

В результате освоения учебной дисциплины у обучающегося должны формироваться профессиональные компетенции, включающие в себя способность:

ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей.

ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.

ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями.

В результате освоения учебной дисциплины у обучающегося должны формироваться общие компетенции, включающие в себя способность:

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем в часах**
Объем образовательной программы	**110**
Во взаимодействии с преподавателем	**104**
лекции	**52**
практические занятия	**52**
Самостоятельная работа	6
Промежуточная аттестация: дифференцированный зачет	

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов междисциплинарного и тем	Содержание учебного материала, практические занятия, самостоятельная работа обучающихся	Объем часов	Формируемые элементы компетенции
1	2	3	4
Раздел 1. Введение и история криптографии		**60**	
Тема 1.1 История криптографии	**Содержание учебного материала**	**6**	
	1. Цели и задачи криптографической защиты информации. Информация и информационная безопасность. Объекты защиты. Категории и носители информации. Средства защиты информации.	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 09, ОК 10, ПК 2.1, ПК2.2, ПК 2.3
	2. Моно-алфавитные подстановочные шифры: Шифр Цезаря, Шифрование Atbash, Аффинный шифр	2	
	3. Шифр ROT 13, Шифр Scytale, Отдельные недостатки подстановки	2	
	Практические занятия:	**4**	
	Практическое занятие № 1 *Отработка шифров Цезаря, Шифрование Atbash, Аффинный шифр*	2	
	Практическое занятие № 2 *Отработка Шифр ROT 13, 47, ASCII ,Шифр Scytale*	2	
Тема 1.2. Мульти-алфавитные подстановочные шифры	**Содержание учебного материала**	**8**	
	4. Шифрование диска, Шифр Виженера .	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 09, ОК 10
	5. Шифр Плейфера, Шифр ADFGVX	2	
	6. Гомофонная замена, Нулевые шифры	2	
	7. Книжные шифры,Шифры Rail Fence, Машина Enigma	2	
Тема 1.3. Симметричная криптография	**Содержание учебного материала**	**42**	
	8 Симметричная криптография: Теория информации, Теоретические основы криптографии.	2	ОК 01, ОК 02, ОК.09
	Практические занятия:	**24**	
	Практическое занятие №3 *Отработка шифров Виженера, Плейфера*	2	ПК 2.1, ПК 2.2, ПК 2.3

	Практическое занятие № 4 *Гомофонная замена, Нулевые шифры*		2	
	Практическое занятие №5 *Отработка книжных шифров, Шифр ADFGVX*		2	
	9.	Принцип Керкхоффса, Подстановка и транспозиция.	2	ОК 01, ОК 02, ОК 09
	10.	Бинарная математика: Двоичное И (AND), Двоичное ИЛИ (OR)	2	
	11.	Двоичное исключающее ИЛИ (XOR), Блочный шифр и потоковый шифр	2	
	12.	Алгоритмы симметричного блочного шифрования: Структура Фейстеля, Несбалансированный шифр Фейстеля	2	
	13.	Стандарт шифрования данных (DES), 3DES	2	
	14.	Стандарт расширенного шифрования (AES): Общий обзор AES, Особенности AES	2	
	15.	Шифры Blowfish, Serpent, Twofish, Skipjack	2	
	16.	Международный алгоритм шифрования данных (IDEA): CAST, TEA, SHARK	2	
	Практическое занятие № 6 Отработка шифра гаммирование: Двоичное И (AND), Двоичное ИЛИ (OR)		2	ПК 2.1, ПК 2.2, ПК 2.3
	Практическое занятие № 7 Отработка шифра Фейстеля		2	
	Практическое занятие № 8 Отработка шифрования данных (DES), 3DES		2	
	Практическое занятие №9 Отработка шифра AES		2	
	Практическое занятие № 10 Отработка шифров Blowfish, Serpent, Twofish, Skipjack		2	
	Практическое занятие № 11 Отработка шифров CAST, TEA, SHARK		2	
	Практическое занятие № 12 Отработка шифров подстановки и транспозиции		2	
	Практическое занятие № 13 Отработка шифра ROT 13, ROT 47 и ASCII		2	
	Практическое занятие №14 Знакомство с инструментом CrypTool		2	
Раздел 2. Симметричные шифры			**18**	
Тема 2.1 Симметричные алгоритмические методы	**Содержание учебного материала**		**4**	ОК01, ОК 02, ОК 03, ОК.04, ОК 05, ОК09, ОК 10, ПК 2.1, ПК 2.2, ПК 2.3
	17.	Электронная кодовая книга (EBC),Cipher-Block Chaining (CBC),Распространение цепочек шифрованных блоков (PCBC).	2	
	18.	Обратная связь с шифрованием (CFB),Обратная связь вывода (OFB),Счетчик (CTR),Вектор инициализации (IV)	2	

Тема 2.2. Симметричные поточные шифры	**Содержание учебного материала**		**4**	
	19.	Пример симметричных поточных шифров: RC , Пример симметричных потоков: FISH	2	
	20.	Пример симметричных поточных шифров: PIKE	2	
Тема 2.3 Функция хеширования	**Содержание**		**10**	
	21.	Хэш и Соль, Алгоритм MD5 MD 6	2	
	22.	Алгоритм безопасного хэша (SHA), FORK-256, RIPEMD-160	2	
	23.	Шифры ГОСТ 28147-89, Tiger, MAC и HMAC	2	
	Практические занятия:		**4**	
	Практическое занятие № 15 Оценка свойств гаммы шифра		2	
	Практическое занятие № 16 Изучение современных поточных криптосистем		2	
Раздел 3. Ассиметричные криптосистемы			**26**	
Тема 3.1 Асимметричная криптография	**Содержание**		**26**	ОК 01, ОК 02, ОК 09
	24.	Простые числа, Относительно простые числа, Функция Эйлера .	2	
	25.	Генерация случайных чисел: Классификация генераторов случайных чисел, Признаки хорошего генератора случайных чисел	2	
	26.	Генератор случайных чисел Лемера, Диффи-Хеллман, Rivest Shamir Adleman (RSA), Цифровая подпись DSA	2	
	Практические занятия:		**20**	
	Практическое занятие №17 Отработка шифров RC , Пример симметричных потоков: FISH		2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 09, ОК 10, ПК 2.1, ПК2.2, ПК 2.3
	Практическое занятие №18 Отработка шифров PIKE		2	
	Практическое занятие №19 Отработка Алгоритмов MD5 MD 6		2	
	Практическое занятие №20 Отработка шифров (SHA), FORK-256, RIPEMD-160		2	
	Практическое занятие №21 Отработка Шифра ГОСТ 28147-89		2	
	Практическое занятие №22 Отработка шифра Лемера		2	
	Практическое занятие №23 Отработка шифра Диффи-Хеллмана		2	
	Практическое занятие №24 Отработка шифра , Rivest Shamir Adleman (RSA		2	
	Практическое занятие №25 Цифровая подпись DSA		2	
	Практическое занятие №26 Схема Эль-Гамаля		2	
Самостоятельная работа			**6**	

Тематика расчетных работ. 1) Режимы блочного шифрования ГОСТ 28147-89, DES. 2) Алгоритм разворачивания ключа шифра AES. 3) Исследование энтропийных свойств русского и английского языков. 4) Построение защитных контрольных сумм на основе бесключевой хэш-функции. 5) Построение криптографической хэш-функции на основе односторонней функции. 6) Построение ключевой информации для ЭЦП. 7) Инфраструктура открытых ключей.		
Во взаимодействии с преподавателем	**104**	
Консультации		
Самостоятельная работа	**6**	
Промежуточная аттестация -диф. зачет		
Объем учебной нагрузки	**110**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Для реализации программы учебной дисциплины предусмотрены следующие специальные помещения.

404. **Лаборатория «Программных и программно-аппаратных средств защиты информации**» оборудована для проведения занятий лекционного типа, практических занятий, лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная оборудованием, техническими средствами обучения и материалами, учитывающими требования международных, национальных и межгосударственных стандартов в области защиты информации.

Перечень основного оборудования, находящегося в кабинете:

- рабочее место преподавателя (стол, стул, персональный компьютер);
- учебная мебель (столы, стулья);
- персональные компьютеры не ниже Core i3;
- коммутатор;
- интерактивная доска;
- проектор;
- аппаратно-программные средства обеспечения разграничения и контроля доступа пользователей АПМДЗ "КРИПТОН-ЗАМОК/К" (М-526А) в комплекте со считывателем смарт карт и устройством для подключения iButton;
- аппаратный шифратор для PC-совместимых компьютеров «КРИПТОН-8/PCI» в комплекте со считывателем смарт карт и устройством для подключения iButton;
- многофункциональный поисковый прибор ST 031 "Пиранья";
- абонентское устройство защиты телефонных линий «Гранит-8»;
- устройство защиты аналогового ТА «МП-1А»;
- устройство защиты цифрового ТА «МП-1А в евророзетке»;
- СИСТЕМНЫЙ КОМПЛЕКТ ARBYTE SILEX M115Q G3/G4400/8GB/4*1TB/RAID ;
- SATA/k+m/2GLAN/500W/minitower;
- ПАК ViPNet IDS100 2.x;
- ПАК ViPNet Coordinator HW50 A 4.x;
- Рутокен PINPad;
- РУТОКЕН ЭЦП 2.0 память 64 Кбайт;
- Рутокен ЭЦП Bluetooth;
- Рутокен S 128КБ;
- USB-токен JaCarta PKI;
- S-Terra.

Используемое программное обеспечение:

- контракт № 29ЭА44-2018 от 06.09.2018 (Лицензия на использование JaCarta Management System от 14.09.2018 серийный номер 96d93439-984b-49be-93e0-db5e33051556 бессрочная, Лицензия на использование Secret Disk Server NG для файлового сервера на 10 пользователей (одновременных подключений) (лицензия сервера - E8E3-5990-3795-131C, лицензия администратора 0AEA-7027-899B-36D1) бессрочная, Передача права на использование ПО ViPNet Client for Windows 4.x (КС2)и ПО ViPNet Administrator 4.x (КС2) рег. Номер № 025-00173 от 21.11.2018 – бессрочная., Лицензия на право использования СКЗИ "КриптоПро CSP" версии 4.0 от 30.08.2018 срок неограничен
- Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. Educational Renewal, срок действия 2 года (Контракт № 20ЭА44-2019 от 29.07.2019);
- ОС Microsoft Windows 10 Professional (предустановленное ПО, Контракт № 64ЭА44-2018 от 09.01.2019 с ООО «Азон», бессрочная);
- 7-Zip (свободно распространяемое ПО);
- Mozilla Firefox (свободно распространяемое ПО);
- Foxit Reader (свободно распространяемое ПО);

- Yandex Browser (свободно распространяемое ПО);
- VSCodium (свободно распространяемое ПО);
- Pinta (свободно распространяемое ПО);
- Adobe Reader (свободно распространяемое ПО);
- LibreOffice (свободно распространяемое ПО).

Электронная библиотечная система IPRbooks (лицензионный договор № 5890/19 от 13 декабря 2019г. с ООО «Ай Пи Ар Медиа» на предоставление доступа к ЭБС IPRbooks, срок действия с 01.01.2020г. по 31.12.2020г.; лицензионный договор № № 7269/20 от 04 декабря 2020 г. с ООО «Ай Пи Ар Медиа» на предоставление доступа к ЭБС IPRbooks, срок действия с 01.01.2021г. по 31.12.2021г.).

Учебно-методическая документация.

219. Кабинет для самостоятельной работы (компьютерный класс), оснащенный компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду.

Перечень основного оборудования, находящегося в кабинете:
- учебная мебель (столы, стулья);
- персональные компьютеры;
- принтеры.

Используемое программное обеспечение:
- Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. Educational Renewal, срок действия 2 года (Контракт № 20ЭА44-2019 от 29.07.2019);
- ОС Astra Linux Common Edition релиз «Орел» (свободно распространяемое ПО);
- 7-Zip (свободно распространяемое ПО);
- Mozilla Firefox (свободно распространяемое ПО);
- Foxit Reader (свободно распространяемое ПО);
- Yandex.Browser (свободно распространяемое ПО);
- VSCodium (свободно распространяемое ПО);
- Pinta (свободно распространяемое ПО);
- AdobeReader (свободно распространяемое ПО);
- LibreOffice (свободно распространяемое ПО).

Электронная библиотечная система IPRbooks (лицензионный договор № 5890/19 от 13 декабря 2019г. с ООО «Ай Пи Ар Медиа» на предоставление доступа к ЭБС IPRbooks, срок действия с 01.01.2020г. по 31.12.2020г.; лицензионный договор № № 7269/20 от 04 декабря 2020 г. с ООО «Ай Пи Ар Медиа» на предоставление до-ступа к ЭБС IPRbooks, срок действия с 01.01.2021г. по 31.12.2021г.).

3.2. Информационное обеспечение обучения

Основная литература:

1. Котов, Ю.А. Криптографические методы защиты информации. Шифры: учебное пособие / Ю. А.Котов. — Новосибирск: Новосибирский государственный технический университет, 2016. — 59 с. — ISBN 978-5-7782-2959-4. — Текст: электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/91377.html

2. Котов, Ю. А. Криптографические методы защиты информации. Стандартные шифры. Шифры с открытым ключом: учебное пособие / Ю. А. Котов. — Новосибирск: Новосибирский государственный технический университет, 2017. — 67 с. — ISBN 978-5-7782-3411-6. — Текст: электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/91227.html

Дополнительная литература:

1. Учебно-методическое пособие по выполнению курсовой работы по дисциплине Криптографические методы защиты информации / составители О.И. Шелухин. — Москва:

Московский технический университет связи и информатики, 2015. — 28 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/63335.html

2. Калмыков, И.А. Криптографические методы защиты информации: лабораторный практикум / И. А. Калмыков, Д. О. Науменко, Т. А. Гиш. — Ставрополь: Северо-Кавказский федеральный университет, 2015. — 109 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/63099.html

3. Практикум по выполнению лабораторных работ по дисциплине Криптографические методы защиты информации / составители А.Э. Смирнов, Ю.А. Пономарёва. — Москва: Московский технический университет связи и информатики, 2015. — 67 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/61738.html

Интернет ресурсы:

http://www.iprbookshop.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Результаты обучения	***Показатели и критерии оценки***	***Формы и методы оценки***
Знания − основные алгоритмы шифрования с секретным и открытым ключом; − криптосистемы на базе алгоритмов Диффи-Хелмана, Эль-Гамаля, RSA, и т.д.; − основные положения криптографических протоколов аутентификации и «электронной подписи». ***Умения*** − производить элементарные операции над шифрами - моно- и многоалфавитные подстановки, системы шифрования Виженера, шифр Плейфера перестановки, гаммирование; − работать со стандартами шифрования DES, блочными шифрами; − использовать алгоритм, криптосистемы без передачи ключей; − составлять протоколы аутентификации; − применять цифровую подпись.	Выполняет простейшие типы шифров. Определяет их достоинства и недостатки, методы реализации. Выполняет методы криптоанализа простейших шифров. Определяет методы криптографической защиты в телекоммуникационных системах и сетях связи. Перечисляет современные методы криптошифров и области применения криптографических средств защиты информации для локальных сетей и открытых. Выполняет и проводит восстановление процесса и параметров функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации. Выполняет администрирование программно-аппаратных средств по обнаружению и выявлению нарушений процессов передачи данных с помощью криптографических средств защиты данных в открытых сетях.	Оценка при выполнении и защите результатов практических занятий. Тестирование. Промежуточная аттестация *(дифференцированный зачет)*

Критерии оценки:

«Отлично» - теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко.

«Хорошо» - теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками.

«Удовлетворительно» - теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки.

«Неудовлетворительно» - теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки