МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования «Вятский государственный университет»
(ВятГУ)
г. Киров

Утверждаю
Директор/Декан *Репкин Д. А.*

Номер регистрации
РПД_3-10.05.02.01_2021_122336
Актуализировано: 11.05.2021

Рабочая программа дисциплины
Методы и средства криптографической защиты информации

наименование дисциплины

Квалификация выпускника	Специалист по защите информации
Специальность	10.05.02 шифр
	Информационная безопасность телекоммуникационных систем наименование
Специализация	Системы подвижной цифровой защищенной связи наименование
Формы обучения	Очная наименование
Кафедра-разработчик	Кафедра радиоэлектронных средств наименование
Выпускающая кафедра	Кафедра радиоэлектронных средств наименование

Киров, 2021 г.

Сведения о разработчиках рабочей программы дисциплины

Харина Наталья Леонидовна

ФИО

Цели и задачи дисциплины

Цель дисциплины	Изучение криптографических методов защиты информации
Задачи дисциплины	- изучение принципов построения криптографических систем - изучение методов оценки криптостойкости криптографических систем - изучение основных принципов и методов криптоанализа криптографических систем - изучение способов генерации ключевых последовательностей - изучение криптографических протоколов (протоколы генерации и распределения ключей, идентификации)

Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Компетенция ОПК-10

Способен использовать методы и средства криптографической защиты информации при решении задач профессиональной деятельности		
Знает	Умеет	Владеет
основные понятия и задачи криптографии в условиях информационного противоборства; основные математические методы, применяемые в алгоритмах шифрования информации; принципы построения криптографических алгоритмов, классификацию алгоритмов современной криптографии; структуру криптографических алгоритмов; требования к шифрам, основные характеристики шифров, модели шифров; роль криптографической защиты информации в комплексе мер по информационной безопасности; основные отечественные и зарубежные стандарты по криптографической защите информации; способы исследования криптоалгоритмов для оценки крипостойкости систем шифрования	представить в формализованном виде итерации криптографических алгоритмов; оценивать математическую сложность алгоритмов асимметричного шифрования данных; применять математические методы, применяемые в алгоритмах шифрования информации; анализировать алгоритмы для определения стойкости к криптоанализу; оценить сложность применения криптографических алгоритмов с точки зрения технической реализуемости; пользоваться сертификатами открытых ключей, применяемых в криптографических системах; анализировать алгоритмы для определения стойкости к криптоанализу	навыками описания структуры современных криптографических алгоритмов; способностью оценки криптостойкости алгоритмов криптозащиты данных; навыками анализа математической сложности алгоритмов шифрования данных; способностью шифрования данных с помощью простых криптоалгоритмов; способностью оценки криптостойкости алгоритмов криптозащиты данных; готовностью применения отечественных и зарубежных стандартов в области криптографии; приемами криптоанализа и криптозащиты сообщений

Структура дисциплины

Тематический план

№ п/п	Наименование разделов дисциплины	Шифр формируемых компетенций
1	Криптографические системы шифрования данных	ОПК-10
2	Криптографические протоколы	ОПК-10
3	Подготовка и прохождение промежуточной аттестации	ОПК-10

Формы промежуточной аттестации

Зачет	Не предусмотрен (Очная форма обучения)
Экзамен	7 семестр (Очная форма обучения)
Курсовая работа	Не предусмотрена (Очная форма обучения)
Курсовой проект	Не предусмотрена (Очная форма обучения)

Трудоемкость дисциплины

Форма обучения	Курсы	Семестры	Общий объем (трудоемкость)		Контактная работа, час	в том числе аудиторная контактная работа обучающихся с преподавателем, час				Самостоятельная работа, час	Курсовая работа (проект), семестр	Зачет, семестр	Экзамен, семестр
			Часов	ЗЕТ		Всего	Лекции	Семинарские, практические занятия	Лабораторные занятия				
Очная форма обучения	4	7	180	5	108.5	72	18	36	18	71.5			7

Содержание дисциплины

Очная форма обучения

Код занятия	Наименование тем занятий	Трудоемкость, академических часов
Раздел 1 «Криптографические системы шифрования данных»		**70.00**
Лекции		
Л1.1	Введение. Требования к криптографическим системам	1.00
Л1.2	Просты алгоритмы шифрования	1.00
Л1.3	Составные алгоритмы шифрования (симметричные криптосистемы)	2.00
Л1.4	Принципы построения асимметричных криптосистем	2.00
Л1.5	Потоковые системы шифрования	1.00
Л1.6	Криптостойкость алгоритмов шифрования	1.00
Семинары, практические занятия		
П1.1	Изучение простых алгоритмов шифрования (перестановка, замена, гаммирование)	2.00
П1.2	Изучение симметричных алгоритмов шифрования (DES, AES, ГОСТ 28147-89, ГОСТ Р 34.12-2015, IDEA, BLOWFISH, RC6)	10.00
П1.3	Изучение асимметричных алгоритмов шифрования (Шамира, RSA, Эль-Гамаля)	2.00
П1.4	Изучение потоковых алгоритмов шифрования (A5, FEAL, RC4)	2.00
П1.5	Оценка стойкости алгоритмов шифрования	2.00
Лабораторные занятия		
Р1.1	Изучение частотного метода криптоанализа шифров замены	4.00
Р1.2	Изучение линейного метода криптоанализа симметричных шифров	4.00
Самостоятельная работа		
С1.1	Изучение алгоритмов шифрования	20.00
Контактная внеаудиторная работа		
КВР1.1	Контактная внеаудиторная работа	16.00
Раздел 2 «Криптографические протоколы»		**83.00**
Лекции		
Л2.1	Изучение алгоритмов вычисления хэш функций	1.00
Л2.2	Протоколы электронной подписи	3.00
Л2.3	Протоколы идентификации	3.00
Л2.4	Протоколы генерации и распределения ключей	3.00
Семинары, практические занятия		
П2.1	Изучение протоколов электронной подписи (RSA, DSA, Эль-Гамаля, ГОСТ-Р.34-94)	6.00
П2.2	Изучение протоколов электронной подписи на эллиптических кривых (ГОСТ Р.34.10-2012)	4.00
П2.3	Изучение протоколов распределения ключей на	2.00

	примере протокола Ментальный покер	
П2.4	Изучение протоколов электронных платежей на основе RSA	4.00
П2.5	Изучение протоколов передачи ключей (алгоритм Диффи-Хеллмана)	2.00
Лабораторные занятия		
Р2.1	Изучение алгоритма электронной подписи (RSA, DSA, ГОСТ 34.10-94)	5.00
Р2.2	Изучение протокола электронной подписи на эллиптических кривых (ГОСТ Р 34.10-2012)	5.00
Самостоятельная работа		
С2.1	Изучение криптографических протоколов	27.00
Контактная внеаудиторная работа		
КВР2.1	Контактная внеаудиторная работа	18.00
Раздел 3 «Подготовка и прохождение промежуточной аттестации»		**27.00**
ЭЗ.1	Подготовка к сдаче экзамена	24.50
КВР3.2	Консультация перед экзаменом	2.00
КВР3.1	Сдача экзамена	0.50
ИТОГО		**180.00**

Содержание дисциплины данной рабочей программы используется при обучении по индивидуальному учебному плану, при ускоренном обучении, при применении дистанционных образовательных технологий и электронном обучении (при наличии).

Методические указания для обучающихся по освоению дисциплины

Успешное освоение дисциплины предполагает активное, творческое участие обучающегося на всех этапах ее освоения путем планомерной, повседневной работы. Обучающийся обязан посещать лекции, семинарские, практические и лабораторные занятия (при их наличии), получать консультации преподавателя и выполнять самостоятельную работу.

Изучение дисциплины следует начинать с проработки настоящей рабочей программы, методических указаний и разработок, указанных в программе, особое внимание уделить целям, задачам, структуре и содержанию дисциплины.

Главной задачей каждой лекции является раскрытие сущности темы и анализ ее основных положений. Тематика лекций определяется настоящей рабочей программой дисциплины.

Лекции – это систематическое устное изложение учебного материала. На них обучающийся получает основной объем информации по каждой конкретной теме. Лекции обычно носят проблемный характер и нацелены на освещение наиболее трудных и дискуссионных вопросов.

Предполагается, что обучающиеся приходят на лекции, предварительно проработав соответствующий учебный материал по источникам, рекомендованным программой. Часто обучающимся трудно разобраться с дискуссионными вопросами, дать однозначный ответ. Преподаватель, сравнивая различные точки зрения, излагает свой взгляд и нацеливает их на дальнейшие исследования и поиск научных решений. После лекции желательно вечером перечитать и закрепить полученную информацию, тогда эффективность ее усвоения значительно возрастает. При работе с конспектом лекции необходимо отметить материал, который вызывает затруднения для понимания, попытаться найти ответы на затруднительные вопросы, используя предлагаемую литературу. Если самостоятельно не удалось разобраться в материале, сформулируйте вопросы и обратитесь за помощью к преподавателю.

Целью семинарских занятий является проверка уровня понимания обучающимися вопросов, рассмотренных на лекциях и в учебной литературе.

Целью практических и лабораторных занятий является формирование у обучающихся умений и навыков применения теоретических знаний в реальной практике решения задач; восполнение пробелов в пройденной теоретической части курса.

Семинарские, практические и лабораторные занятия в равной мере направлены на совершенствование индивидуальных навыков решения теоретических и прикладных задач, выработку навыков интеллектуальной работы, а также ведения дискуссий. Для успешного участия в семинарских, практических и лабораторных занятиях обучающемуся следует тщательно подготовиться.

Основной формой подготовки обучающихся к практическим (лабораторным) занятиям является самостоятельная работа с учебно-методическими материалами, научной литературой, статистическими данными и т.п.

Изучив конкретную тему, обучающийся может определить, насколько хорошо он в ней разобрался. Если какие-то моменты остались непонятными, целесообразно составить список вопросов и на занятии задать их преподавателю. Практические (лабораторные) занятия предоставляют обучающемуся возможность творчески раскрыться, проявить инициативу и развить навыки публичного ведения дискуссий и общения.

Самостоятельная работа обучающихся включает в себя выполнение различного рода заданий (изучение учебной и научной литературы, материалов лекций, систематизацию прочитанного материала, подготовку контрольной работы, решение

задач, подготовка докладов, написание рефератов, публикация тезисов, научных статей, подготовка и защита курсовой работы / проекта и другие), которые ориентированы на глубокое усвоение материала изучаемой дисциплины.

Обучающимся рекомендуется систематически отводить время для повторения пройденного материала, проверяя свои знания, умения и навыки.

Внутренняя система оценки качества освоения дисциплины включает входной контроль уровня подготовленности обучающихся, текущий контроль успеваемости, промежуточную аттестацию, направленную на оценивание промежуточных и окончательных результатов обучения по дисциплине (в том числе результатов курсового проектирования (выполнения курсовых работ) при наличии).

При проведении промежуточной аттестации обучающегося учитываются результаты текущего контроля, проводимого в течение освоения дисциплины.

Процедура оценивания результатов освоения дисциплины осуществляется на основе действующих локальных нормативных актов ФГБОУ ВО «Вятский государственный университет», с которыми обучающиеся ознакамливаются на официальном сайте университета www.vyatsu.ru.

Учебно-методическое обеспечение дисциплины, в том числе учебно-методическое обеспечение самостоятельной работы обучающегося по дисциплине

Учебная литература (основная)

1) Криптографические методы защиты информации. - Санкт-Петербург : ПГУПС, 2018 - . - Текст : электронный.Ч. 2. - Санкт-Петербург : ПГУПС, 2018. - 63 с. - ISBN 978-5-7641-1215-2 : Б. ц. - URL: https://e.lanbook.com/book/138103 (дата обращения: 15.05.2020). - Режим доступа: ЭБС Лань.

2) Рябко, Борис Яковлевич. Криптографические методы защиты информации : учеб. пособие / Б. Я. Рябко, А. Н. Фионов. - 2-е изд. - Москва : Горячая линия-Телеком, 2014. - 229 с. - (Учебное пособие для высших учебных заведений). - Библиогр.: с. 218-222. - ISBN 978-5-9912-0286-2 : 334.95 р. - Текст : непосредственный.

3) Кирпичников, А. П. Криптографические методы защиты компьютерной информации : учебное пособие / А.П. Кирпичников, З.М. Хайбуллина. - Казань : Казанский научно-исследовательский технологический университет (КНИТУ), 2016. - 100 с. : табл., схем. - Библиогр. в кн. - ISBN 978-5-7882-2052-9 : Б. ц. - URL: http://biblioclub.ru/index.php?page=book&id=560536/ (дата обращения: 24.03.2020). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

4) Игнатьев, Е. Б. Основы криптографии : учебное пособие / Е. Б. Игнатьев. - Иваново : ИГЭУ, 2020. - 88 с. - Б. ц. - URL: https://e.lanbook.com/book/154559 (дата обращения: 15.05.2020). - Режим доступа: ЭБС Лань. - Текст : электронный.

5) Основы криптографии : учеб. пособие: специальность 210403 / ВятГУ, ФПМТ, каф.РЭС ; сост. Н. Л. Харина. - Киров : ВятГУ, 2009. - х. - Б. ц. - URL: https://lib.vyatsu.ru. - Режим доступа: для авториз. пользователей. - Текст : электронный.

Учебная литература (дополнительная)

1) 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. : ил., табл. - Библиогр. с 46. - ISBN 978-5-7782-3411-6 : Б. ц. - URL: http://biblioclub.ru/index.php?page=book&id=574782/ (дата обращения: 24.03.2020). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

2) Котов, Ю. А. Криптографические методы защиты информации: шифры : учебное пособие / Ю.А. Котов. - Новосибирск : Новосибирский государственный технический университет, 2016. - 59 с. : ил., табл., граф. - Библиогр. в кн. - ISBN 978-5-7782-2959-4 : Б. ц. - URL: http://biblioclub.ru/index.php?page=book&id=576379/ (дата обращения:

24.03.2020). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

3) Ищукова, Е. А. Криптографические протоколы и стандарты : учебное пособие / Е.А. Ищукова, Е.А. Лобова. - Таганрог : Издательство Южного федерального университета, 2016. - 80 с. : ил. - Библиогр. в кн. - ISBN 978-5-9275-2066-4 : Б. ц. - URL: http://biblioclub.ru/index.php?page=book&id=493059/ (дата обращения: 24.03.2020). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

Учебно-методические издания

1) Криптографические методы защиты информации : лабораторный практикум. - Ставрополь : СКФУ, 2015. - 109 с. - Б. ц. - URL: http://biblioclub.ru/index.php?page=book&id=458059/ (дата обращения: 24.03.2020). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

2) Харина, Наталья Леонидовна. Практикум по основам криптографии / Н. Л. Харина ; ВятГУ, ФПМТ, каф.РЭС. - Киров : ВятГУ, 2009. - х. - Б. ц. - URL: https://lib.vyatsu.ru. - Режим доступа: для авториз. пользователей. - Текст : электронный.

Электронные образовательные ресурсы

1) Портал дистанционного обучения ВятГУ [электронный ресурс] / - Режим доступа: http://mooc.do-kirov.ru/
2) Раздел официального сайта ВятГУ, содержащий описание образовательной программы [электронный ресурс] / - Режим доступа: https://www.vyatsu.ru/php/programms/eduPrograms.php?Program_ID=3-10.05.02.01
3) Личный кабинет студента на официальном сайте ВятГУ [электронный ресурс] / - Режим доступа: https://new.vyatsu.ru/account/
4) Единое окно доступа к образовательным ресурсам http://window.edu.ru/

Электронные библиотечные системы (ЭБС)

- ЭБС «Научная электронная библиотека eLIBRARY» (http://elibrary.ru/defaultx.asp)
- ЭБС «Издательства Лань» (http://e.lanbook.com/)
- ЭБС «Университетская библиотека online» (www.biblioclub.ru)
- Внутренняя электронно-библиотечная система ВятГУ (http://lib.vyatsu.ru/)
- ЭБС «ЮРАЙТ (https://urait.ru)

Современные профессиональные базы данных и информационные справочные системы

- ГАРАНТ
- КонсультантПлюс
- Техэксперт: Нормы, правила, стандарты
- Роспатент (https://www1.fips.ru/elektronnye-servisy/informatsionno-poiskovaya-sistema)
- Web of Science® (http://webofscience.com)

Материально-техническое обеспечение дисциплины

Демонстрационное оборудование

Перечень используемого оборудования
МУЛЬТИМЕДИА ПРОЕКТОР CASIO XJ-A141V С ЭКРАНОМ НАСТЕННЫМ 180*180СМ, ШТАТИВОМ PROFFIX 63-100СМ И КАБЕЛЕМ VGA 15.2М

Специализированное оборудование

Перечень используемого оборудования
ГРАФИЧЕСКАЯ РАБОЧАЯ СТАНЦИЯ DEPO Race X340S
ПЕРСОНАЛЬНЫЙ КОМПЬЮТЕР ICL S253.MI (МОНОБЛОК)
ПЕРСОНАЛЬНЫЙ КОМПЬЮТЕР ICL SafeRay S251.Mi (МОНОБЛОК)

Учебно-наглядное пособие

Перечень используемого оборудования
СОБОЛЬ PCI ВЕРСИЯ 3.0 (ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС С DS-1995)
УЧЕБНО-ЛАБОРАТОРНЫЙ КОМПЛЕКС ДЛЯ ПРОЕКТИРОВАНИЯ И МОДЕЛИРОВАНИЯ АНАЛОГОВЫХ И ЦИФРОВЫХ СХЕМ

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, в том числе лицензионное и свободно распространяемое ПО (включая ПО отечественного производства)

№ п.п	Наименование ПО	Краткая характеристика назначения ПО
1	Программная система с модулями для обнаружения текстовых заимствований в учебных и научных работах «Антиплагиат.ВУЗ»	Программный комплекс для проверки текстов на предмет заимствования из Интернет-источников, в коллекции диссертация и авторефератов Российской государственной библиотеки (РГБ) и коллекции нормативно-правовой документации LEXPRO
2	Microsoft Office 365 ProPlusEdu ALNG SubsVL MVL AddOn toOPP	Набор веб-сервисов, предоставляющий доступ к различным программам и услугам на основе платформы Microsoft Office, электронной почте бизнес-класса, функционалу для общения и управления документами
3	Office Professional Plus 2016	Пакет приложений для работы с различными типами документов: текстами, электронными таблицами, базами данных, презентациями
4	Windows Professional	Операционная система
5	Kaspersky Endpoint Security для бизнеса	Антивирусное программное обеспечение
6	Справочная правовая система «Консультант Плюс»	Справочно-правовая система по законодательству Российской Федерации
7	Электронный периодический справочник ГАРАНТ Аналитик	Справочно-правовая система по законодательству Российской Федерации
8	Security Essentials (Защитник Windows)	Защита в режиме реального времени от шпионского программного обеспечения, вирусов.
9	МойОфис Стандартный	Набор приложений для работы с документами, почтой, календарями и контактами на компьютерах и веб браузерах
10	2009Лицензия на СКЗИ"КриптоПро CSP"версии3.0	Специализированное лицензионное ПО

Обновленный список программного обеспечения данной рабочей программы находится по адресу: https://www.vyatsu.ru/php/list_it/index.php?op_id=122336