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

Утверждаю
Директор/Декан *Бушмелева Н. А.*

Номер регистрации
РПД_3-01.03.02.52_2020_115131
Актуализировано: 22.03.2021

Рабочая программа дисциплины
Криптография

наименование дисциплины

Квалификация выпускника	Бакалавр
Направление подготовки	01.03.02 шифр
	Прикладная математика и информатика наименование
Направленность (профиль)	3-01.03.02.52 шифр
	Математическое и программное обеспечение информационных систем наименование
Формы обучения	Очная наименование
Кафедра-разработчик	Кафедра прикладной математики и информатики (ОРУ) наименование
Выпускающая кафедра	Кафедра прикладной математики и информатики (ОРУ) наименование

Киров, 2020 г.

Сведения о разработчиках рабочей программы дисциплины

Пушкарев Игорь Александрович

ФИО

Цели и задачи дисциплины

Цель дисциплины	Изучить классические и современные криптографические протоколы и способы их использования для решения информационно-правовых задач.
Задачи дисциплины	Освоить основные принципы конструирования и использования криптографических протоколов на практике.

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

Компетенция ПК-3

Способен осуществлять построение концептуальной архитектуры системы, определение ключевых свойств и ограничений системы		
Знает	Умеет	Владеет
основные понятия прикладной математики, использующиеся в криптографии, её методы, место и роль в решении задач защиты информации	объяснять математические основы криптосистем и криптографических протоколов; применять математические методы для решения практических задач защиты информации, работать с современными системами программирования	инструментарием для решения криптографических задач

Компетенция УК-2

Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений		
Знает	Умеет	Владеет
правовые аспекты защиты информации, использования криптографических протоколов; типы и особенности криптосистем	выбирать оптимальный тип криптосистемы с учетом особенностей поставленной задачи защиты информации	навыком применения криптосистем и криптографических протоколов для защиты информации

Структура дисциплины

Тематический план

№ п/п	Наименование разделов дисциплины	Шифр формируемых компетенций
1	История криптографии и классические симметричные криптосистемы	ПК-3, УК-2
2	Асимметричные криптосистемы и протоколы, основанные на них	ПК-3, УК-2
3	Подготовка и прохождение промежуточной аттестации	ПК-3, УК-2

Формы промежуточной аттестации

Зачет	8 семестр (Очная форма обучения)
Экзамен	Не предусмотрен (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	8	144	4	96	60	30	0	30	48		8	

Содержание дисциплины

Очная форма обучения

Код занятия	Наименование тем занятий	Трудоемкость, академических часов
Раздел 1 «История криптографии и классические симметричные криптосистемы»		**50.00**
Лекции		
Л1.1	История криптографии и стеганографии	2.00
Л1.2	Классические симметричные криптосистемы	2.00
Лабораторные занятия		
Р1.1	Шифр Вернама	2.00
Р1.2	Криптосистема Плэйфер	2.00
Р1.3	Перестановочные шифры и композиция шифрований	2.00
Самостоятельная работа		
С1.1	Повторение лекций	11.00
С1.2	Подготовка к лабораторным работам	11.00
Контактная внеаудиторная работа		
КВР1.1	Контактная внеаудиторная работа	18.00
Раздел 2 «Асимметричные криптосистемы и протоколы, основанные на них»		**90.00**
Лекции		
Л2.1	Первые асимметричные криптосистемы: головоломки Меркла и криптосистема, основанная на задаче укладки рюкзака	2.00
Л2.2	Криптосистема RSA	2.00
Л2.3	Цифровые подписи и блобы	1.00
Л2.4	Протоколы обмена ключами	1.00
Л2.5	"Человек посредине" и взаимоблокировка	1.00
Л2.6	Широковещательная передача анонимных сообщений	1.00
Л2.7	Однонаправленных хэш-функции	2.00
Л2.8	Протоколы аутентификации	2.00
Л2.9	Разделение секрета	2.00
Л2.10	Подбрасывание монеты по телефону и покер по телефону	2.00
Л2.11	Протоколы онлайн-голосования	2.00
Л2.12	Цифровые деньги	2.00
Л2.13	Законные криптосистемы	2.00
Л2.14	Схема Рабина	1.00
Л2.15	Схема Эль-Гамаля	1.00
Л2.16	Схема Шнорра	2.00
Лабораторные занятия		
Р2.1	Криптосистема на основе задачи об укладке рюкзака	2.00
Р2.2	Криптосистема RSA	6.00
Р2.3	Однонаправденные хэш-функции	2.00
Р2.4	Электронные подписи	2.00

Р2.5	Доказательства с нулевым разглашением	2.00
Р2.6	Протоколы аутентификации	2.00
Р2.7	Протоколы раззделения секрета	2.00
Р2.8	Схема Рабина	2.00
Р2.9	Схема Эль-Гамаля	2.00
Р2.10	Схема Шнорра	2.00
Самостоятельная работа		
С2.1	Повторение лекций	11.00
С2.2	Подготовка к лабораторным работам	11.50
Контактная внеаудиторная работа		
КВР2.1	Контакнтая внеаудиторная работа	17.50
Раздел 3 «Подготовка и прохождение промежуточной аттестации»		**4.00**
З3.1	Подготовка к сдаче зачета	3.50
КВР3.1	Сдача зачета	0.50
ИТОГО		**144.00**

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) 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.

2) Фергюсон, Нильс. Практическая криптография / Н. Фергюсон, Б. Шнайер. - М. : Диалектика, 2005. - 424 с. : ил. - Библиогр.: с. 410-418. - ISBN 5-8459-0733-0. - ISBN 0-4712-2357-3 : 282.00 р. - Текст : непосредственный.

3) Левин, Максим. Криптография без секретов. Руководство пользователя / М. Левин. - М. : ЗАО "Новый издат. дом", 2005. - 320 с. - Библиогр.: с. 307-308. - ISBN 5-9643-0063-1 : 161.50 р. - Текст : непосредственный.

Учебная литература (дополнительная)

1) Василенко, Олег Николаевич. Теоретико-числовые алгоритмы в криптографии : монография / О. Н. Василенко ; Ин-т проблем информ. безопасности МГУ. - Москва : МЦНМО, 2006. - 336 с. - (Информационная безопасность: криптография). - Библиогр.: с. 303-321. - ISBN 5-94057-103-4 : 150.00 р. - Текст : непосредственный.

2) Рябко, Б. Я. Основы современной криптографии и стеганографии / Б.Я. Рябко. - Москва : Горячая линия - Телеком, 2010. - 232 с. - ISBN 978-5-9912-0150-6 : Б. ц. - URL: http://biblioclub.ru/index.php?page=book&id=253604/ (дата обращения: 24.03.2020). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

3) Лидовский, В. В. Основы теории информации и криптографии : курс / В.В. Лидовский. - Москва : Интернет-Университет Информационных Технологий, 2007. - 125 с. - Б. ц. - URL: http://biblioclub.ru/index.php?page=book&id=234148/ (дата обращения: 24.03.2020). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

4) Романьков, Виталий Анатольевич. Введение в криптографию : учеб. пособие / В. А. Романьков. - 2-е изд., испр. и доп. - Москва : Форум, 2012. - 239, [1] с. - Библиогр.: с. 233-234. - ISBN 978-5-91134-573-0 : 347.00 р. - Текст : непосредственный.

Учебно-методические издания

1) Теоретико-числовые методы в криптографии : практикум. - Ставрополь : СКФУ, 2017. - 107 с. : ил. - Б. ц. - URL: http://biblioclub.ru/index.php?page=book&id=483838/ (дата обращения: 24.03.2020). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

2) Пушкарев, Игорь Александрович. Введение в теорию кодов, исправляющих ошибки и криптографию : учебно-методич. пособие / И. А. Пушкарев ; ВятГУ, ФПМТ, каф. ПМиИ. - Киров : ВятГУ, 2009. - Б. ц. - 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=3-01.03.02.52
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
ПЕРСОНАЛЬНЫЙ КОМПЬЮТЕР ICL RAY S253.Mi (МОНОБЛОК)
ПРОЕКТОР CASIO XJ-F210WN
ЭКРАН ПРОЕКЦИОННЫЙ DIGIS DSOB-1106

Специализированное оборудование

Перечень используемого оборудования
ПЕРСОНАЛЬНЫЙ КОМПЬЮТЕР ICL RAY S253.Mi (МОНОБЛОК)

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	Visual Studio Community	Интегрированная среда разработки ПО

Обновленный список программного обеспечения данной рабочей программы находится по адресу: https://www.vyatsu.ru/php/list_it/index.php?op_id=115131