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_3-44.03.05.66_2017_116464
Актуализировано: 29.03.2021

Рабочая программа дисциплины
Основы криптографии

наименование дисциплины

Квалификация выпускника	Бакалавр пр.
Направление подготовки	44.03.05 шифр
	Педагогическое образование (с двумя профилями подготовки) ФКиФМН наименование
Направленность (профиль)	3-44.03.05.66 шифр
	Физика, информатика наименование
Формы обучения	Очная наименование
Кафедра-разработчик	Кафедра прикладной математики и информатики (ОРУ) наименование
Выпускающая кафедра	Кафедра физики и методики обучения физике (ОРУ) наименование

Киров, 2017 г.

Сведения о разработчиках рабочей программы дисциплины

Разова Елена Владимировна

ФИО

Цели и задачи дисциплины

Цель дисциплины	формирование у обучающихся знаний в области криптографии и навыков практического обеспечения защиты информации, подготовка студентов к решению практических задач, которые могут возникнуть у них в процессе дальнейшего образования и практической деятельности
Задачи дисциплины	• изучение основ защиты информации; • изучение основных угроз; • изучение использования криптографических преобразований для защиты информации; • получение представления о типовых криптографических средствах защиты информации и возможностях их использования; • знакомство с направлениями наиболее эффективного решения криптографических задач; • формирование умений и навыков по эффективному применению средств вычислительной техники; • обучение самостоятельному поиску и использованию нормативно-технической и справочной литературы и электронных источников информации.

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

Компетенция ПК-4

способностью использовать возможности образовательной среды для достижения личностных, метапредметных и предметных результатов обучения и обеспечения качества учебно-воспитательного процесса средствами преподаваемых учебных предметов		
Знает	Умеет	Владеет
правовые аспекты защиты информации; основные понятия, методы криптографии, ее роль в защите информации; виды криптографических систем	объяснять математические основы криптосистем и криптографических протоколов; устанавливать межпредметные связи математики и информатики при описании и применении криптографических методов защиты информации и обосновании их криптостойкости	навыком применения криптосистем и криптографических протоколов для защиты информации

Структура дисциплины

Тематический план

№ п/п	Наименование разделов дисциплины	Шифр формируемых компетенций
1	Общие принципы защиты информации	ПК-4
2	Криптографические методы защиты информации	ПК-4
3	Подготовка и прохождение промежуточной аттестации	ПК-4

Формы промежуточной аттестации

Зачет	Не предусмотрен (Очная форма обучения)
Экзамен	10 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	5	10	144	4	73.5	38	18	0	20	70.5			10

Содержание дисциплины

Очная форма обучения

Код занятия	Наименование тем занятий	Трудоемкость, академических часов
Раздел 1 «Общие принципы защиты информации»		**20.00**
Лекции		
Л1.1	Введение в методы защиты информации	2.00
Л1.2	Угрозы	2.00
Самостоятельная работа		
С1.1	Проработка материала лекций. Знакомство с правовыми аспектами защиты информации	8.00
Контактная внеаудиторная работа		
КВР1.1	Контактная внеаудиторная работа	8.00
Раздел 2 «Криптографические методы защиты информации»		**97.00**
Лекции		
Л2.1	Симметричные шифры: блочные шифры (Lucifer, DES, 3DES, ГОСТ, AES, IDEA) поточные шифры (A5, RC4)	4.00
Л2.2	Хеширование	2.00
Л2.3	Алгоритм Диффи-Хеллмана. Асимметричные шифры (RSA). Цифровая подпись	2.00
Л2.4	Сетевые атаки. Протокол IPSec. Протокол SSH.	2.00
Л2.5	Аутентификация. Многоразовые и одноразовые пароли. Протокол Kerberos. Биометрическая аутентификация	2.00
Л2.6	Сертификаты. Протоколы TLS/SSL. Атаки	2.00
Лабораторные занятия		
Р2.1	Криптографические системы с симметричным ключом. Поточные шифры	2.00
Р2.2	Криптографические системы с симметричным ключом. Блочные шифры	4.00
Р2.3	Ассиметричные криптосистемы	4.00
Р2.4	Хранение паролей, хеширование	2.00
Р2.5	Электронно-цифровая подпись	4.00
Р2.6	Обеспечение безопасности передачи данных и безопасности удаленных подключений	4.00
Самостоятельная работа		
С2.1	Проработка материала лекций	12.00
С2.2	Подготовка отчетов о выполнении заданий лабораторных работ	26.00
Контактная внеаудиторная работа		
КВР2.1	Контактная внеаудиторная работа	25.00
Раздел 3 «Подготовка и прохождение промежуточной аттестации»		**27.00**
Э3.1	Подготовка к сдаче экзамена	24.50
КВР3.1	Консультация перед экзаменом	2.00
КВР3.2	Сдача экзамена	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) Басалова, Г. В. Основы криптографии : курс лекций / Г.В. Басалова. - Москва : Интернет-Университет Информационных Технологий, 2011. - 253 с. - Б. ц. - URL: http://biblioclub.ru/index.php?page=book&id=233689/ (дата обращения: 24.03.2020). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

2) 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.

3) 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.

Учебная литература (дополнительная)

1) Кнауб, Л. В. Теоретико-численные методы в криптографии : учебное пособие / Л.В. Кнауб. - Красноярск : Сибирский федеральный университет, 2011. - 160 с. - ISBN 978-5-7638-2113-7 : Б. ц. - URL: http://biblioclub.ru/index.php?page=book&id=229582/ (дата обращения: 24.03.2020). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

2) Каширская, Е. Н. Основы криптографического анализа : учебное пособие / Е. Н. Каширская. - Москва : РТУ МИРЭА, 2020. - 74 с. - Б. ц. - URL: https://e.lanbook.com/book/163805 (дата обращения: 15.05.2020). - Режим доступа: ЭБС Лань. - Текст : электронный.

3) Каширская, Е. Н. Криптографический анализ и методы защиты информации : учебное пособие / Е. Н. Каширская. - Москва : РТУ МИРЭА, 2020. - 91 с. - Б. ц. - URL: https://e.lanbook.com/book/163861 (дата обращения: 15.05.2020). - Режим доступа: ЭБС Лань. - 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.

Учебно-наглядное пособие

РПД_3-44.03.05.66_2017_116464

1) Исупова, Татьяна Николаевна. Обеспечение безопасности в информационной образовательной среде : учебное наглядное пособие для бакалавров направления подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки), Безопасность жизнедеятельности, дополнительное образование / Т. Н. Исупова ; ВятГУ, ИМИС, ФКиФМН, каф. ЦТО. - Киров : ВятГУ, 2021. - 28 с. - Б. ц. - Текст . Изображение : электронное.

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=3-44.03.05.66
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
Блок системный
Настенный экран Luma 198x264
Проектор №2

Специализированное оборудование

Перечень используемого оборудования
ПЕРСОНАЛЬНЫЙ КОМПЬЮТЕР ICL SafeRay S251.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=116464