Министерство науки и высшего образования РФ
Федеральное государственное автономное образовательное учреждение высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.ДВ.03.02 Cryptographic methods for data protection

наименование дисциплины (модуля) в соответствии с учебным планом

Направление подготовки / специальность

09.04.03 Прикладная информатика

Направленность (профиль)

09.04.03.08 Технологии цифровой экономики

Форма обучения очная

Год набора 2021

СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ | SIBERIAN FEDERAL UNIVERSITY
ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 6EA1 7389 2A8A 5ACD E60C 3E69 C5A6 A666
Владелец: ФГАОУ ВО "СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ"
Действителен: с 24 мая 2022 г по 17 августа 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Программу составили _____

канд. экон. наук, Руйга Ирина Рудольфовна

должность, инициалы, фамилия

1 Цели и задачи изучения дисциплины

1.1 Цель преподавания дисциплины

Дисциплина «Криптографические методы защиты информации» предусмотрена учебным планом программы по направлению 09.04.03 «Прикладная информатика», магистерская программа «Технологии цифровой экономики». Целью изучения дисциплины является формирование у будущих выпускников теоретических знаний в области основополагающих принципов защиты информации с помощью криптографических методов и приобретение практических навыков реализации этих методов на практике.

1.2 Задачи изучения дисциплины

Задачами изучения дисциплины являются:

- изучение основных понятий, методологии и практических приемов управления аппаратными и программными средствами защиты информации;
- приобретение студентами необходимого объема знаний и практических навыков в области стандартизации и нормотворчества в управлении информационной безопасностью, аппаратными и программными средствами защиты информации, организации работы и разграничения полномочий персонала, ответственного за информационную безопасность и программные средства, реализующие различные криптографические функции.

1.3 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Код и наименование индикатора достижения компетенции	Запланированные результаты обучения по дисциплине
ПК-1: Способен использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС	
ПК-1.1: Знает: методы анализа результатов исследований в области интеллектуального анализа данных; стандарты проектно-технологической документации; методики подготовки принятия решений	- методологии и технологии реинжиниринга, проектирования и аудита прикладных информационных систем различных классов; - методы научных исследований и инструментария в области проектирования и управления ИС; - методы анализа данных, необходимых для решения поставленных задач. - обосновывать архитектуру ИС; - принимать решения по информатизации предприятий в условиях неопределенности;выбирать методологию и технологию проектирования информационных систем; - управлять проектами ИС на всех стадиях ее жизненного цикла, оценивать эффективность и качество проекта; - выбирать инструментальные средства для обработки данных в соответствии с поставленной задачей. - навыками управления проектами по

	информатизации прикладных процессов и систем; - навыками управления информационными ресурсами и сервисами с использованием современных инструментальных средств; - навыками реинжиниринга прикладных и информационных процессов; - навыками моделирования процессов и ИС.
ПК-1.2: Умеет: использовать типовые программные продукты для исследования экспериментальных данных; разрабатывать практические рекомендации по повышению эффективности применения методов интеллектуального анализа данных; формировать перечень параметров выбора проектных решений	
ПК-1.3:	
УК-4: Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	

УК-4.1: Знать: современные коммуникативные технологии на государственном и иностранном языках; закономерности деловой устной и письменной коммуникации	— современные средства информационнокоммуникационных технологий; – языковой материал (лексические единицы и грамматические структуры), необходимый и достаточный для общения в различных средах и сферах речевой деятельности. — воспринимать на слух и понимать содержание аутентичных общественнополитических, публицистических (медийных) и прагматических текстов, относящихся к различным типам речи, выделять в них значимую информацию; — понимать содержание научнопопулярных и научных текстов, блогов/веб-сайтов; — выделять значимую информацию из прагматических текстов справочноинформационного и рекламного характера; — вести диалог, соблюдая нормы речевого этикета, используя различные стратегии; выстраивать монолог; — составлять деловые бумаги, в том числе оформлять CurriculumVitae/Resume и сопроводительное письмо, необходимые при приеме на работу; — вести запись основных мыслей и фактов (из аудиотекстов и текстов для чтения), запись тезисов устного выступления/письменного доклада по изучаемой проблеме; — поддерживать контакты при помощи электронной почты.
	— практическими навыками использования современных коммуникативных технологий; – грамматическими категориями изучаемого (ых) иностранного (ых) языка (ов).
УК-4.2: Уметь: применять на практике коммуникативные технологии, методы и способы делового общения	
УК-4.3: Владеть методикой межличностного делового общения на государственном и иностранном языках, с применением профессиональных языковых форми средств	

1.4 Особенности реализации дисциплины

Язык реализации дисциплины: .

Дисциплина (модуль) реализуется с применением ЭО и ДОТ

URL-адрес и название электронного обучающего курса: .

2. Объем дисциплины (модуля)

Вид учебной работы	Всего, зачетных единиц (акад.час)	е
		1
Контактная работа с преподавателем:	**1,33 (48)**	
занятия лекционного типа	0,44 (16)	
практические занятия	0,89 (32)	
Самостоятельная работа обучающихся:	**2,67 (96)**	
курсовое проектирование (КП)	Нет	
курсовая работа (КР)	Нет	
Промежуточная аттестация (Экзамен)	**1 (36)**	

3 Содержание дисциплины (модуля)

3.1 Разделы дисциплины и виды занятий (тематический план занятий)

№ п/п	Модули, темы (разделы) дисциплины	Контактная работа, ак. час.							
		Занятия лекционного типа		Занятия семинарского типа				Самостоятельная работа, ак. час.	
				Семинары и/или Практические занятия		Лабораторные работы и/или Практикумы			
		Всего	В том числе в ЭИОС	Всего	В том числе в ЭИОС	Всего	В том числе в ЭИОС	Всего	В том числе в ЭИОС
1. Введение в криптографию. История криптографии. Исторические шифры.									
	1. Понятие и содержание информационной безопасности (основные определения, подходы к определению, классификация угроз; информационная безопасность в системе национальной безопасности)	1							
	2. Понятие и содержание информационной безопасности (основные определения, подходы к определению, классификация угроз; информационная безопасность в системе национальной безопасности)			2					
	3. Классификация средств защиты информации. Методы и средства организационно-правовой защиты информации. Методы и средства инженерно-технической защиты	2							

4. Классификация средств защиты информации. Методы и средства организационно-правовой защиты информации. Методы и средства инженерно-технической защиты			2					
5. Введение в криптографию. История криптографии. Исторические шифры	1							
6. Введение в криптографию. История криптографии. Исторические шифры			4					
7. Введение в криптографию. История криптографии. Исторические шифры. Introduction to Cryptography. History of cryptography. Historical ciphers							24	
2. Математическая модель шифра. Теория секретности Шеннона. Блочные шифры. Псевдослучайные последовательности и								
1. Математическая модель шифра. Теория секретности Шеннона. Блочные шифры	2							
2. Математическая модель шифра. Теория секретности Шеннона. Блочные шифры			4					
3. Псевдослучайные последовательности и поточные шифры	2							
4. Псевдослучайные последовательности и поточные шифры			4					
5. Теория имитостойкости Симмонса и криптографические хэш-функции	2							
6. Теория имитостойкости Симмонса и криптографические хэш-функции			4					

7. Математическая модель шифра. Теория секретности Шеннона. Блочные шифры. Псевдослучайные последовательности и поточные шифры. Теория имитостойкости Симмонса и криптографические хэш-функции. Mathematical model of the cipher. Shannon's theory of secrecy. Block ciphers. Pseudo-random sequences and stream ciphers. Simmons impersonation theory and cryptographic hash functions							36	
3. Асимметричные (с открытым ключом) шифры. Схемы цифровой подписи. Введение в криптографические протоколы.								
1. Основные понятия и классификация средств ассиметричной криптографической защиты информации. Требования к алгоритмам шифрования с открытым ключом	2							
2. Основные понятия и классификация средств ассиметричной криптографической защиты информации. Требования к алгоритмам шифрования с открытым ключом			4					
3. Общая схема электронной цифровой подписи. Использование хеш-функций. Виды асимметричных алгоритмов цифровой подписи	2							
4. Общая схема электронной цифровой подписи. Использование хеш-функций. Виды асимметричных алгоритмов цифровой подписи			4					
5. Электронная подпись на основе алгоритма RSA. Цифровая подпись на основе алгоритма Эль-Гамаля. Стандарты на алгоритмы цифровой подписи	2							

6. Электронная подпись на основе алгоритма RSA. Цифровая подпись на основе алгоритма Эль-Гамаля. Стандарты на алгоритмы цифровой подписи			4					
7. Асимметричные (с открытым ключом) шифры. Схемы цифровой подписи. Введение в криптографические протоколы. Asymmetric (with public key) ciphers. Digital signature schemes. An introduction to cryptographic protocols							36	
Всего	16		32				96	

4 Учебно-методическое обеспечение дисциплины

4.1 Печатные и электронные издания:

1. Громов Ю. Ю., Драчев В. О., Иванова О. Г., Шахов Н. Г. Основы информационной безопасности: учебное пособие для студентов вузов по направлению "Информационные системы и технологии"(Старый Оскол: ТНТ).
2. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации: Учебное пособие(Москва: Издательский Центр РИО□).
3. Солдатова Г. У., Рассказова Е. И., Нестик Т. А. Цифровое поколение России: компетентность и безопасность: [монография](Москва: Смысл).

4.2 Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства (программное обеспечение, на которое университет имеет лицензию, а также свободно распространяемое программное обеспечение):

1. Microsoft Windows (7, 8 или 10 версия)
2. Microsoft Office Professional Plus 2007
3. Google Chrome Free

4.3 Интернет-ресурсы, включая профессиональные базы данных и информационные справочные системы:

1. Каждый обучающийся в течение всего периода обучения по дисциплине обеспечен индивидуальным неограниченным доступом к электронно-библиотечным системам (электронным библиотекам) и к электронной информационно-образовательной среде Университета (Электронно-библиотечная система СФУ. – Режим доступа: http://bik.sfu-kras.ru/).
2. Электронно-библиотечная система (электронная библиотека) и электронная информационно-образовательная среда обеспечивают возможность доступа для обучающегося из любой точки, в которой имеется доступ к сети Интернет, и отвечают техническим требованиям организации, как на территории Университета, так и вне ее.
3. Электронная информационно-образовательная среда Университета обеспечивает:
4. доступ к учебным планам, рабочим программам дисциплин (модулей), практик, и к изданиям электронных библиотечных систем и электронным образовательным ресурсам, указанным в рабочих программах;
5. фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения основной образовательной программы;
6. проведение всех видов занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных образовательных технологий;

7. формирование электронного портфолио обучающегося, в том числе сохранение работ обучающегося, рецензий и оценок на эти работы со стороны любых участников образовательного процесса;
8. взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействие посредством сети Интернет.

5 Фонд оценочных средств

Оценочные средства находятся в приложении к рабочим программам дисциплин.

6 Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)

Для проведения занятий лекционного типа требуется наличие аудитории, оборудованной специализированной учебной мебелью, панелью интерактивной жидкокристаллической или проектором, доской маркерной.

Для проведения практических занятий требуется наличие аудитории, оборудованной специализированной учебной мебелью, доской маркерной или меловой.

Помещения для самостоятельной работы обучающихся должны быть оснащены компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду Университета.