Минобрнауки России

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой

Сирота Александр Анатольевич

Кафедра технологий обработки и защиты информации

29.06.2021

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.ДВ.06.02 Криптография и стеганография

1. Код и наименование направления подготовки/специальности:

09.03.02 Информационные системы и технологии

2. Профиль подготовки/специализация:

Информационные системы в телекоммуникациях, Обработка информации и машинное обучение, Программная инженерия в информационных системах, Информационные системы и сетевые технологии, Информационные системы и технологии в управлении предприятием

3. Квалификация (степень) выпускника:

Бакалавриат

4. Форма обучения:

Очная

5. Кафедра, отвечающая за реализацию дисциплины:

Кафедра технологий обработки и защиты информации

6. Составители программы:

Дрюченко Михаил Анатольевич, к.т.н., доцент

7. Рекомендована:

протокол № 5 от 10.03.21

8. Учебный год:

2023-2024

9.Цели и задачи учебной дисциплины:

Изучение математических основ криптографической защиты информации, вопросов обеспечения конфиденциальности, целостности, аутентичности данных, использование криптографических средств для решения задач идентификации и аутентификации, изучение криптографических протоколов, рассмотрение вопросов моделирования случайных величин с заданным законом распределения, изучение принципов криптоанализа, изучение методов стеганографии и стегоанализа, получение профессиональных компетенций в области современных технологий защиты информации.

Основные задачи дисциплины:

- обучение студентов математическим основам криптографии, базовым принципам работы симметричных и ассиметричных криптографических систем при использовании специализированных протоколов и программных средств шифрования данных;

- обучение студентов базовым принципам создания электронных цифровых подписей при решении задач аутентификации;
- обучение студентов базовым принципам стеганографического сокрытия информации и создания цифровых водяных знаков;

овладение практическими навыками применения теоретических знаний для контроля целостности, шифрования конфиденциальной информации, решения задач идентификации и аутентификации.

10. Место учебной дисциплины в структуре ООП:

Дисциплина относится к вариативной части профессионального цикла дисциплин по выбору учебного плана.

Входные знания в области информатики, теории информации, математической статистики, цифровой обработки сигналов, навыки программирования.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников) и индикаторами их достижения:

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ПКВ-3 Способен выполнять работы по созданию (модификации) и сопровождению информационных систем	ПКВ-3.1 Знает языки и методы программирования, инструменты и методики тестирования разрабатываемых ИС	Знает современные языки программирования, возможности современных программных сред и специализированных библиотек для разработки программных средств защиты конфиденциальности информации, контроля целостности и аутентификации данных. Умеет разрабатывать и применять на практике специализированные криптографические и стеганографические программные средства в интересах обеспечения безопасности и целостности данных.
ПКВ-3 Способен выполнять работы по созданию (модификации) и сопровождению информационных систем	ПКВ-3.2 Знает устройство и функционирование современных ИС, протоколы, интерфейсы и форматы обмена данными	Знает принципы работы и устройство современых криптографических и стеганографических алгоритмов и протоколов. Владеет практическими навыками примения современых криптографических и стеганографических алгоритмов и протоколов.

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ПКВ-1 Способен проводить исследования на всех этапах жизненного цикла программных средств	ПКВ-1.1 Знает методы и средства планирования и организации исследований и разработок	Знает базовые принципы работы криптографических методов для решения задач защиты конфиденциальности, аутентичности и целостности данных, механизмы генерации, хранения и использования криптографических ключей. Умеет планировать и проводить исследования специализированного программного обеспечения в части корректного выбора криптографиических методов и алгоритмов, механизмов работы с ключевой информацией
ПКВ-1 Способен проводить исследования на всех этапах жизненного цикла программных средств	ПКВ-1.2 Знает методы проведения экспериментов и наблюдений, обобщения и обработки информации	Знает базовые принципы проведения экспериментов и наблюдений, обобщения и обработки информации. Владеет практическими навыками проведения исследований по учету исполнения требований безопасности информации на всех этапах жизненного цикла специализированных криптографических и стеганографических программных средств
ПКВ-1 Способен проводить исследования на всех этапах жизненного цикла программных средств	ПКВ-1.3 Планирует отдельные стадии исследования или разработки при наличии поставленной задачи, выбирает или формирует программную среду для компьютерного моделирования и проведения экспериментов	Знает основные стадии разработки ПО, принципы декомпозиции задач, возможности современных программных сред и специализированных библиотек для разработки программных средств защиты конфиденциальности информации, контроля целостности данных. Умеет выбирать программные средства и библиотеки для реализации, моделирования и исследования криптографических и стеганографических алгоритмов.

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ПКВ-1 Способен проводить исследования на всех этапах жизненного цикла программных средств	ПКВ-1.4 Использует стандартное и оригинальное программное обеспечение и проводит компьютерный эксперимент, составляет его описание и формулирует выводы	Знает основные стадии разработки ПО, принципы декомпозиции задач, возможности современных программных сред и специализированных библиотек для разработки программных средств защиты конфиденциальности информации, контроля целостности данных. Умеет проводить экспериментальные исследования криптографических и стеганографических алгоритмов и специализированных программных компонент. Владеет навыками составления аналитических отчетов по результатам проведенных экспериментов.
ПКВ-1 Способен проводить исследования на всех этапах жизненного цикла программных средств	ПКВ-1.5 Обрабатывает полученные результаты исследований с использованием стандартных методов (методик)	Знает аспекты корректного использования криптографических и стеганографических алгоритмов при разработке и сопровождении специализированного ПО. Владеет навыками обработки полученных результатов исследовния криптографических и стеганографических алгоритмов.

12. Объем дисциплины в зачетных единицах/час:

4/144

Форма промежуточной аттестации:

Экзамен

13. Трудоемкость по видам учебной работы

Вид учебной работы	Семестр 5	Всего
Аудиторные занятия	50	50
Лекционные занятия	34	34
Практические занятия	16	16
Лабораторные занятия		0
Самостоятельная работа	58	58
Курсовая работа		0
Промежуточная аттестация	36	36
Часы на контроль	36	36
Всего	144	144

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1.1	Введение. Теоретические аспекты криптографии	1. Исторические сведения и этапы развития криптографии. Предметная область криптографии. Математические основы криптографии. 2. Моделирование случайных величин с заданным законом распределения. Датчики случайных чисел.	Создан онлан электронный курс, размещены материалы к лекции. Размещены индивидуальные задания для выполнения лабораторных работ.
1.2	Криптографические методы и стандарты	3. Симметричные криптосистемы. 4. Блочные шифры. 5. Симметричное поточное шифрование. 6. Асимметричные криптосистемы. 7. Хэш-функции, принципы использования хэш-функций для обеспечения целостности данных. 8. Электронная цифровая подпись (ЭЦП). 9. Криптография с использованием эллиптических кривых. Шифрование, обмен ключами, ЭЦП на основе эллиптических кривых. 10. Квантовая криптография. 11. Виды криптоанализа. Базовые принципы работы криптоаналитических алгоритмов.	Создан онлан электронный курс, размещены материалы к лекции. Размещены индивидуальные задания для выполнения лабораторных работ.
1.3	Стеганографические методы	12. Предметная область стеганографии. Цифровая и компьютерная стеганография 13. Методы и алгоритмы стеганографического встраивания данных в пространственном представлении контейнеров. 14. Методы и алгоритмы стеганографического встраивания данных в частотном представлении контейнеров. 15. Методы стегоанализа.	Создан онлан электронный курс, размещены материалы к лекции. Размещены индивидуальные задания для выполнения лабораторных работ.

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
2. Практические занятия			
2.1	Введение. Теоретические аспекты криптографии	1. Практическое изучение принципов работы датчиков псевдо-случайных числовых последовательностей. Реализация датчиков ПСЧП. Примеры решения задачи.	Размещены индивидуальные задания для выполнения лабораторных работ.

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
2.2	Криптографические методы и стандарты	2. Практическое изучение особенностей работы одного из методов построения блочных шифров – сети Фейстеля. Реализация сети Фейстеля заданной архитектуры. Примеры решения задачи. 3. Изучение различных режимов работы блочных алгоритмов симметричного шифрования. Модификация ранее реализованной сети Фейстеля для работы в режимах ECB, CBC, OFB. Примеры решения задачи. 4. Практическое изучение алгоритмов хеширования на основе блочных алгоритмов шифрования. Модификация ранее реализованного блочного алгоритма шифрования для создания алгоритма хеширования. Примеры решения задачи. 5. Практическое изучение алгоритмов асимметричного шифрования. Реализация алгоритма RSA. Примеры решения задачи. 6. Практическое изучение возможностей и особенностей работы с известными криптографическими библиотеками (cryptopp). Настройка и компиляция модулей библиотеки, подключение к тестовому проекту и использование необходимых функций (выработки ключей на основе текстовых строк PBKDF2, хеширования SHA-1, симметричного шифрования AES и т.д.). Примеры решения задачи. 7. Практическое изучение принципов частотного криптоанализа. Реализация алгоритма для дешифровки закрытых текстов на русском и английском языках, созданных с использованием простейших шифров моноалфавитной подстановки. Примеры решения задачи.	Размещены индивидуальные задания для выполнения лабораторных работ.

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
2.3	Стеганографические методы	8. Практическое изучение алгоритмов стеганографического встраивания в пространственное представление контейнеров-изображений. Примеры решения задачи. 9. Практическое изучение алгоритмов стеганографического встраивания в спектральное представление контейнеров-изображений. Примеры решения задачи.	Размещены индивидуальные задания для выполнения лабораторных работ.
3. Лабораторные работы			
3.1	нет		

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
1	Введение. Теоретические аспекты криптографии	4	2		6	12
2	Криптографические методы и стандарты	22	8		32	62
3	Стеганографические методы	8	6		20	34
		34	16	0	58	108

14. Методические указания для обучающихся по освоению дисциплины

1) При изучении дисциплины рекомендуется использовать следующие средства**:**

- рекомендуемую основную и дополнительную литературу;
- методические указания и пособия;
- контрольные задания для закрепления теоретического материала;
- электронные версии учебников и методических указаний для выполнения лабораторно - практических работ (при необходимости материалы рассылаются по электронной почте).

2) Для максимального усвоения дисциплины рекомендуется проведение письменного опроса (тестирование, решение задач) студентов по материалам лекций и практических работ. Подборка вопросов для тестирования осуществляется на основе изученного теоретического материала.

Такой подход позволяет повысить мотивацию студентов при конспектировании лекционного материала.

3) При проведении практических занятий обеспечивается максимальная степень соответствия с материалом лекционных занятий и осуществляется экспериментальная проверка методов, алгоритмов и технологий обработки информации, излагаемых в рамках лекций.

4) При использовании дистанционных образовательных технологий и электронного обучения выполнять все указания преподавателей, вовремя подключаться к online занятиям, ответственно подходить к заданиям для самостоятельной работы

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

№ п/п	Источник
1	*Дрюченко, Михаил Анатольевич. Методы и алгоритмы стеганографического скрытия и создания цифровых водяных знаков : учебное пособие / М.А. Дрюченко, Е.Ю. Митрофанова ; Воронеж. гос. ун-т .— Воронеж : Издательский дом ВГУ, 2019 .— 144 с. : ил., цв. ил. — ISBN 978-5-9273-2747-8.*
2	*Криптография и стеганография в информационных технологиях / Б.Я. Рябко, А.Н. Фионов, Ю.И. Шокин ; Рос. акад. наук, Сиб. отд-ние, Ин-т вычисл. технологий СО РАН .— Новосибирск : Наука, 2015 .— 239 с. : ил. — Библиогр.: с.232-236 .— ISBN 978-5-02-019206-5.*
3	*Круглов И.А. Введение в теоретико-числовые методы криптографии / И.А. Круглов [и др.]. – СПб: Лань, 2011. – 400 с.*
4	Криптографические методы защиты информации [Электронный ресурс] : учебно-методическое пособие : [для студ. фак. прикладной математики, информатики и механики очной и очно-заоч. форм обучения, для направлений и специальностей: 01.03.02 - Прикладная математика и информатика, 02.03.02 - Фундаментальная информатика и информационные технологии, 01.04.02 - Прикладная математика и информатика, 10.05.01 - Компьютерная безопасность] / Воронеж. гос. ун-т ; сост.: Б.Н. Воронков, Ю.А. Крыжановская .— Электрон. текстовые дан. — Воронеж : Издательский дом ВГУ, 2018 .— Загл. с титул. экрана .— Свободный доступ из интрасети ВГУ .— Текстовый файл .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/m18-241.pdf>.

б) дополнительная литература:

№ п/п	Источник
1	*Щербаков, Андрей Юрьевич. Современная компьютерная безопасность. Теоретические основы. Практические аспекты : учебное пособие для студ. вузов / А.Ю. Щербаков .— М. : Кн. мир, 2009 .— 351, [1] с. : ил., табл. — (Высшая школа) .— Библиогр.: с.350-351 .— ISBN 978-5-8041-0378-2.*
2	Криптографические методы защиты информации : учебное пособие для вузов / Воронеж. гос. ун-т; сост. Б.Н. Воронков .— Воронеж : ИПЦ ВГУ, 2008 .— 58 с. : ил .— Библиогр.: с.52-58 .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/m08-17.pdf>.

№ п/п	Источник
3	Шифрование. Кодирование. Архивация [Электронный ресурс] : учебно-методическое пособие для вузов : [для студ. 2-го к. днев. отд-ния фак. приклад. математики, информатики и механики ; для специальности 080500.62 -Бизнес-информатика] / Воронеж. гос. ун-т ; сост. Ю.А. Крыжановская .— Электрон. текстовые дан. — Воронеж : Издательско-полиграфический центр Воронежского государственного университета, 2013 .— Загл. с титула экрана .— Свободный доступ из интрасети ВГУ .— Текстовый файл .— Windows 2000; Adobe Acrobat Reader .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/m13-218.pdf>.
4	Чмора А.Л. Современная прикладная криптография (учебное пособие для ВУЗов) / А.Л. Чмора. – М.: Гелиос АРВ, 2002 – 244с.
5	Теоретические основы компьютерной безопасности (учебное пособие для ВУЗов) / П.Н. Девянин [и др.]. – М.: Радио и связь, 2000 – 192с.
6	Круглов И.А. Введение в теоретико-числовые методы криптографии / И.А. Круглов [и др.]. – СПб: Лань, 2011. – 400 с.

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
1	*Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/).*
2	*Образовательный портал «Электронный университет ВГУ».– (https://edu.vsu.ru/)*
3	ЭБС «Издательства «Лань», Договор №3010-06/71-14 от 25.11.2014, ЭБС «Университетская библиотека online», Договор №3010-06/70-14 от 25.11.14, Национальный цифровой ресурс «РУКОНТ», Договор №ДС-208 от 01.02.2012

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Криптографические методы защиты информации [Электронный ресурс] : учебно-методическое пособие : [для студ. фак. прикладной математики, информатики и механики очной и очно-заоч. форм обучения, для направлений и специальностей: 01.03.02 - Прикладная математика и информатика, 02.03.02 - Фундаментальная информатика и информационные технологии, 01.04.02 - Прикладная математика и информатика, 10.05.01 - Компьютерная безопасность] / Воронеж. гос. ун-т ; сост.: Б.Н. Воронков, Ю.А. Крыжановская .— Электрон. текстовые дан. — Воронеж : Издательский дом ВГУ, 2018 .— Загл. с титула экрана .— Свободный доступ из интрасети ВГУ .— Текстовый файл .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/m18-241.pdf>.

№ п/п	Источник
2	*Криптографические методы защиты информации : учебное пособие для вузов / Воронеж. гос. ун-т; сост. Б.Н. Воронков .— Воронеж : ИПЦ ВГУ, 2008 .— 58 с. : ил .— Библиогр.: с.52-58 .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/m08-17.pdf>.*

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение):

Для реализации учебного процесса используются:

ПО Microsoft в рамках подписок «Imagine», ежегодные сублицензионные договоры № 56035/BPH3739 и № 56036/BPH3739 от 07.10.2016.

При проведении занятий в дистанционном режиме обучения используются технические и информационные ресурсы Образовательного портала "Электронный университет ВГУ (https:\\edu.vsu.ru), базирующегося на системе дистанционного обучения Moodle, развернутой в университете.

18. Материально-техническое обеспечение дисциплины:

1) Мультимедийная лекционная аудитория (корп.1а, ауд. № 479), ПК-Intel-i3, рабочее место преподавателя: проектор, видеокоммутатор, микрофон, аудиосистема, специализированная мебель: доски меловые 2 шт., столы 60 шт., лавки 30 шт., стулья 64 шт.; доступ к фондам учебно-методической документации и электронным библиотечным системам, выход в Интернет.

2) Компьютерный класс (один из №1-4 корп. 1а, ауд. № 382-385), ПК-Intel-i3 16 шт., специализированная мебель: доска маркерная 1 шт., столы 16 шт., стулья 33 шт.; доступ к фондам учебно-методической документации и электронным изданиям, доступ к электронным библиотечным системам, выход в Интернет.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
1	Разделы 1-3 Введение. Теоретические аспекты криптографии. Криптографические методы и стандарты. Стеганографические методы.	ПКВ-3	ПКВ-3.1	Контрольная работа по соответствующим разделам. Практические работы.

№ п/п	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
2	Разделы 1-3 Введение. Теоретические аспекты криптографии. Криптографические методы и стандарты. Стеганографические методы.	ПКВ-3	ПКВ-3.2	Контрольная работа по соответствующим разделам. Практические работы.
3	Разделы 1-3 Введение. Теоретические аспекты криптографии. Криптографические методы и стандарты. Стеганографические методы.	ПКВ-1	ПКВ-1.1	Контрольная работа по соответствующим разделам. Практические работы.
4	Разделы 1-3 Введение. Теоретические аспекты криптографии. Криптографические методы и стандарты. Стеганографические методы.	ПКВ-1	ПКВ-1.2	Контрольная работа по соответствующим разделам. Практические работы.
5	Разделы 1-3 Введение. Теоретические аспекты криптографии. Криптографические методы и стандарты. Стеганографические методы.	ПКВ-1	ПКВ-1.3	Контрольная работа по соответствующим разделам. Практические работы.
6	Разделы 1-3 Введение. Теоретические аспекты криптографии. Криптографические методы и стандарты. Стеганографические методы.	ПКВ-1	ПКВ-1.4	Контрольная работа по соответствующим разделам. Практические работы.
7	Разделы 1-3 Введение. Теоретические аспекты криптографии. Криптографические методы и стандарты. Стеганографические методы.	ПКВ-1	ПКВ-1.5	Контрольная работа по соответствующим разделам. Практические работы.

Промежуточная аттестация

Форма контроля - Экзамен

Оценочные средства для промежуточной аттестации

Перечень вопросов, практическое задание

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах устного опроса (индивидуальный опрос, фронтальная беседа) и письменных работ (контрольные, лабораторные работы). При оценивании могут использоваться количественные или качественные шкалы оценок.
Текущий контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:
Устный опрос на практических занятиях;
Контрольная работа по теоретической части курса;
Практические работы.

Примерный перечень применяемых оценочных средств

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	Устный опрос на практических занятиях	Вопросы по темам/разделам дисциплины	Правильный ответ – зачтено, неправильный или принципиально неточный ответ - не зачтено
2	Контрольная работа по разделам дисциплины	Теоретические вопросы по темам/разделам дисциплины	Шкала оценивания соответствует приведенной ниже
3	Практическая работа	Содержит 9 практических заданий, предусматривающих разработку, тестирование и эксплуатацию различных криптографических и стеганографических алгоритмов.	При успешном выполнении работы ставится оценка зачтено и осуществляется допуск к экзамену, в противном случае ставится оценка не зачтено и обучающийся не допускается к экзамену.

Пример задания для выполнения практической работы

Практическая работа №2

«Блочное симметричное шифрование»

Цель работы:

Практическое изучение особенностей работы одного из методов построения блочных шифров – сети Фейстеля.

Форма контроля:

Опрос в устной форме по исходному коду и результатам работы реализованной программы.

Количество отведённых аудиторных часов: 4

Содержание работы:

Получить у преподавателя вариант задания, написать код, реализующий соответствующий алгоритм обработки информации. Провести тестирование реализованного алгоритма при различных значениях параметров. Проанализировать полученные результаты и сформулировать выводы по проделанной работе.

Пример варианта задания:

Реализовать процедуры шифрования и расшифровки информации с использованием сети Фейстеля заданной архитектуры (рисунок 1). Размер шифруемого блока 64 бита (b=6), размеры подблоков [x] и [x] по 32 бита. Секретный ключ [x] – случайная 64-битная последовательность. Раундовые ключи $K_i = (K >>> i*3)_{0..31}$, $i = \overline{0,n-1}$. Число раундов [x] изменяется от 2 до 12. Образующая функция $F(L_i, K_i) = (L_i <<< 9) \oplus (\sim((K_i >>> 11) \otimes L_i))$, $i = \overline{0,n-1}$. Исследовать влияние параметров сети на качество получаемых зашифрованных последовательностей.

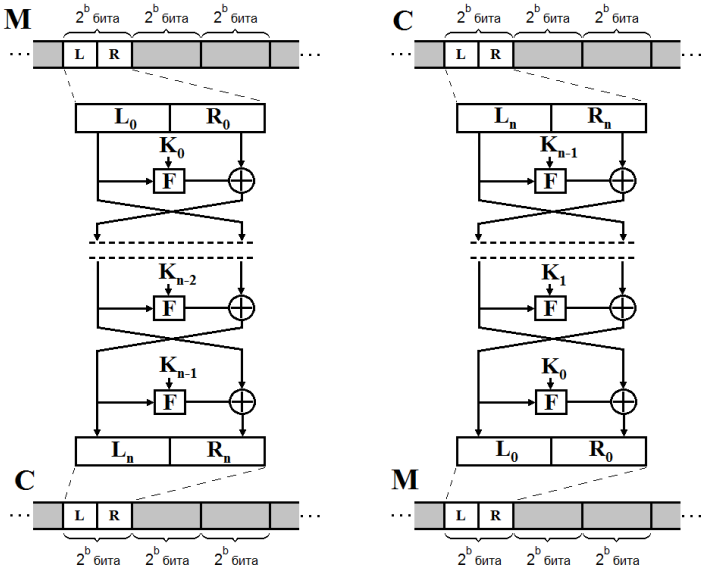

Рисунок 1

Примеры контрольных вопросов:

1. На примере своего варианта реализации практического задания пояснить свойства симметричности и обратимости сети Фейстеля.

2. Каким способом достигаются эффекты рассеивания и перемешивания?

Пример заданий теста по разделам дисциплины

1	Максимальная длина ключа в алгоритме Blowfish *а) 512 бит* *б) 128 бит* *в) 256 бит* *г) 448 бит*	

2	Задачей дискретного логарифмирования является *а) нахождение степени, в которую следует возвести простое число для получения заданного целого числа* *б) нахождение степени, в которую следует возвести целое число для получения заданного целого числа* *в) разложение числа на простые сомножители*	
3	Какой из алгоритмов реализует асимметричное шифрование и м. использоваться для ЭП *а) 3DES* *б) Blowfish* *в) AES* *г) RSA*	
4	Хеш-функция должна обладать следующими свойствами *а) для любого данного значения хеш-кода h вычислительно невозможно най ти M такое, что H (M) = h* *б) хеш-функция H должна применяться к блоку данных фиксированной длины* *в) хеш-функция H создает выход фиксированной длины* *г) хэш-функция H должна создавать выход произвольной длины* *д) для любого данного x вычислительно невозможно найти y ≠ x, что H(y) = H(x)* *е) для любого данного x вычислительно невозможно найти H (x)*	
...	...	

20.2 Промежуточная аттестация

Промежуточная аттестация может включать в себя проверку теоретических вопросов, а также, при необходимости (в случае невыполнения в течение семестра), проверку выполнения установленного перечня практических работ, позволяющих оценить уровень полученных знаний и/или практическое (ие) задание(я), позволяющее (ие) оценить степень сформированности умений и навыков.

Для оценки теоретических знаний используется перечень контрольно-измерительных материалов. Каждый контрольно-измерительный материал для проведения промежуточной аттестации включает два задания - вопросов для контроля знаний, умений и владений в рамках оценки уровня сформированности компетенции. При оценивании используется количественная шкала. Критерии оценивания приведены в таблице ниже.

Для оценивания результатов обучения на экзамене используются следующие содержательные показатели (формулируется с учетом конкретных требований дисциплины):

1. знание теоретических основ учебного материала, основных определений, понятий и используемой терминологии;
2. умение проводить обоснование и представление основных теоретических и практических результатов (теорем, алгоритмов, методик) с использованием математических выкладок, блок-схем, структурных схем и стандартных описаний к ним;
3. умение связывать теорию с практикой, иллюстрировать ответ примерами, в том числе,

собственными, умение выявлять и анализировать основные закономерности, полученные, в том числе, в ходе выполнения практических заданий;
4. умение обосновывать свои суждения и профессиональную позицию по излагаемому вопросу;
5. владение навыками программирования;
6. владение навыками проведения компьютерного эксперимента, тестирования компьютерных моделей алгоритмов обработки информации.

Различные комбинации перечисленных показателей определяют критерии оценивания результатов обучения (сформированности компетенций) на государственном экзамене:

- высокий (углубленный) уровень сформированности компетенций;
- повышенный (продвинутый) уровень сформированности компетенций;
- пороговый (базовый) уровень сформированности компетенций.

Для оценивания результатов обучения на государственном экзамене используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Для оценивания результатов обучения на зачете используется – зачтено, не зачтено по результатам тестирования.

Соотношение показателей, критериев и шкалы оценивания результатов обучения на государственном экзамене представлено в следующей таблице.

Критерии оценивания компетенций и шкала оценок на экзамене

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся демонстрирует полное соответствие знаний, умений, навыков по приведенным критериям свободно оперирует понятийным аппаратом и приобретенными знаниями, умениями, применяет их при решении практических задач. Успешно выполнены практические работы в соответствии с установленным перечнем.	Повышенный уровень	Отлично
Ответ на контрольно-измерительный материал не полностью соответствует одному из перечисленных выше показателей, но обучающийся дает правильные ответы на дополнительные вопросы. При этом обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач. Успешно выполнены практические работы в соответствии с установленным перечнем.	Базовый уровень	Хорошо
Обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач. При этом ответ на контрольно-измерительный материал не соответствует любым двум из перечисленных показателей, обучающийся дает неполные ответы на дополнительные вопросы. Успешно выполнены практические работы в соответствии с установленным перечнем.	Пороговый уровень	Удовлетворительно

Ответ на контрольно-измерительный материал не соответствует любым трем из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки. Не выполнены практические работы в соответствии с установленным перечнем.	–	Неудовлетворительно

Примерный перечень вопросов к экзамену

№	Содержание
1	Алгоритмы симметричного шифрования
2	Криптосистемы с открытым ключом, однонаправленные функции
3	Режимы выполнения алгоритмов симметричного шифрования (ECB, CBC, CFB, OFB)
4	*Прямая и арбитражная ЭП*
5	*Электронная подпись*
6	*Однонаправленные хэш-функции.*
7	*Алгоритм шифрования RSA*
8	*Схема распределения ключей Диффи-Хеллмана на основе эллиптических кривых.*
9	*Алгоритм шифрования DES, тройной DES*
10	*Алгоритм электронной подписи на основе эллиптических кривых ECDSA*
11	*Алгоритм шифрования Эль-Гамаля*
12	Криптография с использованием эллиптических кривых
13	*Алгоритм шифрования Blowfish*
14	*Квантовая криптография*
15	*Алгоритм хеширования MD5*
16	Сеть Фейстеля
17	*Система распределения ключей Диффи-Хеллмана*
18	*Нелинейные регистры сдвига с обратной связью*
19	Гаммирование, линейный регистр сдвига с обратной связью
20	Программные датчики ПСП чисел

21	Предметная область стеганографии. Классификация стеосистем
22	Алгоритмы создания цифровых водяных знаков
22	Алгоритмы стеганографического скрытия информации в пространственном представлении контейнеров-изображений
23	Алгоритмы стеганографического скрытия информации в частотном представлении контейнеров-изображений
24	Алгоритмы стегоанализа

Пример контрольно-измерительного материала

УТВЕРЖДАЮ

Заведующий кафедрой технологий обработки и защиты информации

_____ А.А. Сирота

__.__.2021

Направление подготовки / специальность 09.03.02 Информационные системы и технологии

Дисциплина Б1.В.ДВ.06.01 Криптография и стеганография

Форма обучения Очное

Вид контроля Экзамен

Вид аттестации Промежуточная

Контрольно-измерительный материал № 1

1. Режимы выполнения алгоритмов симметричного шифрования (ECB, CBC, CFB, OFB)

2. Система распределения ключей Диффи-Хеллмана

Преподаватель _____ М.А. Дрюченко