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

Сирота А.А.

12.07.2021г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.О.24 Информационная безопасность

1. Код и наименование направления подготовки/специальности:

09.03.03 Прикладная информатика

2. Профиль подготовки/специализация:

Прикладная информатика в экономике

3. Квалификация выпускника:

Бакалавриат

4. Форма обучения:

Очная

5. Кафедра, отвечающая за реализацию дисциплины:

Кафедра технологий обработки и защиты информации

6. Составители программы:

Иванков Александр Юрьевич, к.ф.-м.н., доцент

7. Рекомендована:

Протокол НМС ФКН №5 от 10.03.21

8. Учебный год: 2024-2025 **Семестр(ы)/Триместр(ы):** 8

9. **Цели и задачи учебной дисциплины**

Целями освоения учебной дисциплины являются:

Изучение теоретических основ информационной безопасности, защиты информации от несанкционированного доступа, обеспечения конфиденциальности обмена информацией в информационно-вычислительных системах, вопросов защиты исходных и байт кодов программ; овладение практическими навыками применения методов криптографии, стеганографии, получение профессиональных компетенций в области современных технологий защиты информации.

Задачи учебной дисциплины:

- обучение студентов теоретическим и практическим аспектам обеспечения информационной безопасности;
- обучение студентов базовым принципам защиты конфиденциальной информации, методам идентификации, аутентификации пользователей информационной системы, принципам организации скрытых каналов передачи информации, принципам защиты авторских прав на объекты цифровой интеллектуальной собственности;
- овладение практическими навыками применения теоретических знаний для шифрования конфиденциальной информации, стеганографического скрытия информации, контроля за целостностью информации, решения задач идентификации и аутентификации.

10. Место учебной дисциплины в структуре ООП:

Входит в блок обязательных дисциплин Б1.О.

Входные знания в области устройства ЭВМ и операционных систем, принципах их работы, сетевых технологий, информатики.

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

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1	Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Знать: основные теоретические и практические аспекты обеспечения информационной безопасности, основные требования к обеспечению информационной безопасности, в том числе защите государственной тайны.
		ОПК-3.2	Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Уметь: применять на практике теоретические знания в области криптографии и стеганографии.
		ОПК-3.3	Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных до-	Владеть: практическими навыками разработки и применения в профессиональной деятельности

			кладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	криптографических и стеганографических алгоритмов.
ОПК-4	Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	ОПК-4.1	Знает основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы	Знать: методы и средства защиты конфиденциальности информации, методы контроля целостности и аутентификации данных, принципы организации скрытых каналов передачи информации.
		ОПК-4.2	Умеет применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.	Уметь: разрабатывать и применять на практике специализированные программные средства в интересах обеспечения безопасности и целостности данных.
		ОПК-4.3	Владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы.	Владеть: практическими навыками применения специализированных программных средств, предназначенных для обеспечения безопасности и целостности данных.

12. Объем дисциплины в зачетных единицах/час. — 2/72.

Форма промежуточной аттестации зачет с оценкой.

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость			
		Всего	По семестрам		
			№ семестра 8	№ семестра	…
Аудиторные занятия		60	60		
в том числе:	лекции	48	48		
	практические				
	лабораторные	12	12		
Самостоятельная работа		12	12		
в том числе: курсовая работа (проект)					
Форма промежуточной аттестации *(экзамен – __час.)*					
Итого:		72	72		

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК*
1. Лекции			
1.1	Основы государственной информационной политики и информационной безопасности Российской Федерации	Понятие национальной безопасности. Информационная безопасность в системе национальной безопасности Российской Федерации. Государственная информационная политика. Информационные ресурсы. Проблемы информационной войны. Проблемы информационной безопасности в сфере государственного и муниципального управления.	Создан электронный курс, размещены материалы к лекции.

1.2	Информационная безопасность автоматизированных систем	Современная постановка задачи защиты информации. Организационно-правовое обеспечение, информационной безопасности. Информационные системы. Угрозы информации. Методы и модели оценки уязвимости информации.	Создан электронный курс, размещены материалы к лекции.
1.3	Методы и модели оценки уязвимости информации	Эмпирический подход к оценке уязвимости информации. Система с полным перекрытием. Практическая реализация модели «угроза - защита».	Создан электронный курс, размещены материалы к лекции.
1.4	Рекомендации по использованию моделей оценки уязвимости информации	Рекомендации по использованию моделей оценки уязвимости информации	Создан электронный курс, размещены материалы к лекции.
1.5	Методы определения требований к защите информации	Методы определения требований к защите информации	Создан электронный курс, размещены материалы к лекции.
1.6	Функции и задачи защиты информации	Общие положения. Методы формирования функций защиты. Классы задач защиты информации. Функции защиты. Состояния и функции системы защиты информации	Создан электронный курс, размещены материалы к лекции.
1.7	Стратегии защиты информации	Стратегии защиты информации.	Создан электронный курс, размещены материалы к лекции.
1.8	Способы и средства защиты информации	Способы и средства защиты информации.	Создан электронный курс, размещены материалы к лекции.
1.9	Криптографические методы защиты информации	Требования к криптосистемам. Основные алгоритмы шифрования. Цифровые подписи. Криптографические хеш-функции. Криптографические генераторы случайных чисел. Обеспечиваемая шифром степень защиты. Криптоанализ и атаки на криптосистемы. Цифровые водяные знаки (ЦВЗ), виды реализации, практические области применения.	Создан электронный курс, размещены материалы к лекции.
1.10	Архитектура систем защиты информации	Требования к архитектуре СЗИ. Построение СЗИ. Ядро системы защиты информации. Ресурсы системы защиты информации.	Создан электронный курс, размещены материалы к лекции.
2. Практические занятия			
3. Лабораторные занятия			
3.1	Криптографические методы защиты информации	1. Практическое изучение работы алгоритмов блочного симметричного шифрования. 2. Изучение криптографических генераторов случайных чисел. 3. Практическое изучение работы асимметричных алгоритмов шифрования. 4. Изучение частотных характеристик текстовых сообщений. 5. Изучение алгоритмов стеганографического скрытия данных в пространственной и частотной области контейнеров (на примере цифровых изображений). 6. Практическое изучение принципов и методов стегоанализа (на примере визуального и статистического стегоанализа цифровых изображений).	Создан электронный курс. Размещены индивидуальные задания для выполнения лабораторных работ.

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (количество часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
1	Основы государственной информационной политики и информационной безопасности Российской Федерации	8				8
2	Информационная безопасность автоматизированных систем	4				4
3	Методы и модели оценки уязвимости информации	4				4
4	Рекомендации по использованию моделей оценки уязвимости информации	2				2
5	Методы определения требований к защите информации	2				2
6	Функции и задачи защиты информации	4				4
7	Стратегии защиты информации	4				4
8	Способы и средства защиты информации	4				4
9	Криптографические методы защиты информации	12		12	12	36
10	Архитектура систем защиты информации	4				4
	Итого:	48		12	12	72

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 лабораторных 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 переходе на дистанционный режим обучения для создания электронных курсов, чтения лекций он-лайн и проведения лабораторно- практических занятий используется информационные ресурсы Образовательного портала "Электронный университет ВГУ (https:\\edu.vsu.ru), базирующегося на системе дистанционного обучения Moodle, развернутой в университете.

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

а) основная литература:

№ п/п	Источник
1	Филиппов, Б.И. Информационная безопасность. Основы надежности средств связи : учебник / Б.И. Филиппов, О.Г. Шерстнева. – Москва ; Берлин : Директ-Медиа, 2019. – 241 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=499170
2	Баранова, Елена Константиновна. Информационная безопасность и защита информации : учебное пособие : [для студ., обучающихся по направлению "Прикладная информатика"] / Е.К. Баранова, А.В. Бабаш .— 4-е изд. перераб. и доп. — Москва : РИОР : ИНФРА-М, 2019 .— 334, [1] с. : ил., табл. — (Высшее образование) .— Библиогр.: с. 327-330.

б) дополнительная литература:

№ п/п	Источник
1	Элементы теории чисел и критозащита : учебное пособие / Воронеж. гос. ун-т; сост. : Б.Н. Воронеков, А.С. Щеголеватых .— Воронеж : ИПЦ ВГУ, 2008 .— 87 с. : ил .— Библиогр.: с.87 .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/m08-95.pdf>.
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>.
3	Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: СОЛОН-Пресс, 2002. – 272 с.
4	*Теоретические основы компьютерной безопасности (учебное пособие для ВУЗов) / П.Н. Девянин [и др.]. – М.: Радио и связь, 2000 – 192с.*

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет)*:

№ п/п	Ресурс
1	Электронный каталог Научной библиотеки Воронежского государственного университета. – (https://www.lib.vsu.ru/).
2	Образовательный портал «Электронный университет ВГУ».– (https://edu.vsu.ru/)
3	— «Университетская библиотека online» - Контракт № 3010-06/05-20 от 28.12.2020 — «Консультант студента» - Контракт № 3010-06/06-20 от 28.12.2020 — ЭБС «Лань» - Контракт №3010-06/03-21 от 10.03.2021 — «РУКОНТ» (ИТС Контекстум) - Договор ДС-208 от 01.02.2021

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Основы информационной безопасности [Электронный ресурс] : учеб. пособие / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов .— М. : Горячая линия – Телеком, 2011 .— 559 с. : ил. — ISBN 5-93517-292-5 .— ISBN 978-5-93517-292-5 .— Режим доступа: https://rucont.ru/efd/202786

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

Для реализации учебного процесса используются:

1 клиентские и серверные ОС и ПО Microsoft в рамках подписок <Imagine>. 3-летняя подписка по договору 3010-16/96-18 от 29.12.2018

2 ПО Dr. Web Enterprise Security Suite Комплексная защита Dr. Web Desktop Security Suite + Центр управления на 12 месяцев, 1400 ПК (Продление) договор 3010-07/01-19 от 09.01.19

3 Университетская лицензия на программный комплекс для ЭВМ MathWorks MATLAB Total Academic Headcount - 25 по договору 3010-07/01-19 от 09.01.19

4 ПО XSpider, лицензия на 16 хостов, сертифицированная версия, акт предоставления прав N Pr000778 от 05.06.2018

5 Лицензия на право использования СКЗИ <КриптоПро Рутокен CSP>, акт предоставления прав N Pr000778 от 05.06.2018

6 Академическая лицензия (на 5 лет) на Учебно-методический комплекс <Программно-аппаратная защита сетей с защитой от НСД> в составе: ПО ViPNet Administrator 4.x - 2 шт., ПО ViPNet Coordinator Windows 4.x - 2 шт., ПО ViPNet Coordinator Linux - 2 шт., ПО ViPNet Client 4.x - 20 шт., ПО ViPNet Policy Manager 4.x - 1 шт., 1 узел управления Policy Manager - 20 шт., ПО ViPNet StateWatcher 4.x - 1 шт., 1 узел мониторинга StateWatcher - 20 шт.

7 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. № 297), ПК-Intel-G3420, рабочее место преподавателя: проектор, видеокоммутатор, специализированная мебель: доска меловая 1 шт., столы 31 шт., стулья 64 шт.; выход в Интернет, доступ к фондам учебно-методической документации и электронным изданиям.
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	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1.	Разделы 1-10 Основы государственной информационной политики и информационной безопасности Российской Федерации. Информационная безопасность автоматизированных систем. Методы и модели оценки уязвимости информации. Рекомендации по использованию моделей оценки уязвимости информации. Методы определения требований к защите информации. Функции и задачи защиты информации. Стратегии защиты информации. Способы и средства защиты информации. Криптографические методы защиты информации. Архитектура систем защиты информации.	ОПК-3	ОПК-3.1	Собеседование, контрольная работа по соответствующим разделам. Лабораторные работы 1-6.
2.	Разделы 1-10	ОПК-3	ОПК-3.2	Собеседование, контрольная работа по соответствующим разделам.

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
	Основы государственной информационной политики и информационной безопасности Российской Федерации. Информационная безопасность автоматизированных систем. Методы и модели оценки уязвимости информации. Рекомендации по использованию моделей оценки уязвимости информации. Методы определения требований к защите информации. Функции и задачи защиты информации. Стратегии защиты информации. Способы и средства защиты информации. Криптографические методы защиты информации. Архитектура систем защиты информации.			Лабораторные работы 1-6.
3.	Разделы 1-10 Основы государственной информационной политики и информационной безопасности Российской Федерации. Информационная безопасность автоматизированных систем. Методы и модели оценки уязвимости информации. Рекомендации по использованию моделей оценки уязвимости информации. Методы определения требований к защите информации. Функции и задачи защиты информации. Стратегии защиты информации. Способы и средства защиты информации. Криптографические методы защиты информации. Архитектура систем защиты информации.	ОПК-3	ОПК-3.3	Собеседование, контрольная работа по соответствующим разделам. Лабораторные работы 1-6.
4.	Разделы 1-10 Основы государственной информационной политики и информационной безопасности Российской Федерации. Информационная безопасность автоматизированных систем. Методы и модели оценки уязвимости информации. Рекомендации по использованию моделей оценки уязвимости информации. Методы определения требований к защите информации. Функции и задачи защиты информации. Стратегии защиты информации. Способы и средства защиты информации. Криптографические методы защиты информации. Архитектура систем защиты информации.	ОПК-4	ОПК-4.1	Собеседование, контрольная работа по соответствующим разделам. Лабораторные работы 1-6.

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
5.	Разделы 1-10 Основы государственной информационной политики и информационной безопасности Российской Федерации. Информационная безопасность автоматизированных систем. Методы и модели оценки уязвимости информации. Рекомендации по использованию моделей оценки уязвимости информации. Методы определения требований к защите информации. Функции и задачи защиты информации. Стратегии защиты информации. Способы и средства защиты информации. Криптографические методы защиты информации. Архитектура систем защиты информации.	ОПК-4	ОПК-4.2	Собеседование, контрольная работа по соответствующим разделам. Лабораторные работы 1-6.
6.	Разделы 1-10 Основы государственной информационной политики и информационной безопасности Российской Федерации. Информационная безопасность автоматизированных систем. Методы и модели оценки уязвимости информации. Рекомендации по использованию моделей оценки уязвимости информации. Методы определения требований к защите информации. Функции и задачи защиты информации. Стратегии защиты информации. Способы и средства защиты информации. Криптографические методы защиты информации. Архитектура систем защиты информации.	ОПК-4	ОПК-4.3	Собеседование, контрольная работа по соответствующим разделам. Лабораторные работы 1-6.
Промежуточная аттестация форма контроля – зачет с оценкой				

20. Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

Примерный перечень применяемых оценочных средств

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	2	3	4
1	Устный опрос	Вопросы по темам/разделам дисциплины	Шкала оценивания соответствует приведенной в разделе 20.2
2	Контрольная работа по разделам дисциплины	Теоретические вопросы по темам/разделам дисциплины	Шкала оценивания соответствует приведенной в разделе 20.2
3	Лабораторная работа	Содержит 6 лабораторных заданий, предусматриваю-	При успешно выполнении работы осуществляется допуск к

		щих разработку и тестирование криптографических и стеганографических алгоритмов	контрольной работе, в противном случае обучающийся не допускается к контрольной работе.
4	КИМ промежуточной аттестации	Каждый контрольно- измерительный материал для проведения промежуточной аттестации включает 2 вопроса для контроля знаний, умений и владений в рамках оценки уровня сформированности компетенции.	Шкалы оценивания приведены в разделе 20.2

20.1. Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

Пример задания для выполнения лабораторной работы
Лабораторная работа №3
«Изучение асимметричных алгоритмов шифрования»

Цель работы:

Изучение работы асимметричных алгоритмов шифрования на примере алгоритма RSA.

Форма контроля: *отчёт в электронном виде*

Количество отведённых аудиторных часов: *4*

Задание:

Получите у преподавателя вариант задания и напишите код, реализующий заданный алгоритм. Составьте отчёт о проделанной работе, в котором отразите следующие пункты:

1. ФИО исполнителя и номер группы.
2. Название и цель лабораторной работы.
3. Номер своего варианта.
4. Код, написанный исполнителем.
5. Результаты работы программы.

Примеры контрольных вопросов:

1. На чем основывается надежность алгоритма RSA?
2. Какие преобразования лежат в основе криптосистем с открытым ключом?

Пример варианта задания:

Провести дешифрование текста, зашифрованного алгоритмом RSA, на основе известного открытого ключа Kp и шифрованного текста C.

Kp = {n=471090785117207; e=12377}

C = 3149991122810652053617063415173219874910986 67.

Описание технологии проведения

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

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.

Требования к выполнению заданий (или шкалы и критерии оценивания)

При оценивании используется количественная шкала. Критерии оценивания приведены выше в таблице раздела 20.2.

20.2. Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств:

Примерный перечень вопросов к зачету

№	Содержание
1	Основы государственной информационной политики и информационной безопасности Российской Федерации
2	Угрозы информационной безопасности, модели нарушителей
3	Методы и модели оценки уязвимости информации
4	Рекомендации по использованию моделей оценки уязвимости информации
5	Функции и задачи защиты информации
6	Предметная область криптографии
7	Алгоритмы симметричного шифрования, сеть Фейстеля
8	Режимы выполнения алгоритмов симметричного шифрования (ECB, CBC, CFB, OFB)
9	Криптосистемы с открытым ключом, однонаправленные функции

10	Однонаправленные хэш-функции
11	Электронная подпись
12	Программные датчики ПСП чисел
13	Принципы работы криптоаналитических алгоритмов.
14	Предметная область стеганографии
15	Стеганографическое скрытие данных в пространственной области контейнера
16	Стеганографическое скрытие данных в частотной области контейнера, методы кодирования с расширением спектра
17	Статистические и структурные методы скрытия информации
18	Цифровые водяные знаки
19	Стегоанализ. Визуальный, статистический, универсальный стегоанализ.
20	Архитектура систем защиты информации
21	Общие требования к построению надежной системы защиты

Пример контрольно-измерительного материала

УТВЕРЖДАЮ

Заведующий кафедрой технологий обработки и защиты информации

_____ А.А. Сирота

__.__.2021

Направление подготовки / специальность 09.03.03 Прикладная информатика

Дисциплина Б1.О.24 Информационная безопасность

Форма обучения Очное

Вид контроля Зачет с оценкой

Вид аттестации Промежуточная

Контрольно-измерительный материал № 1

1. Режимы выполнения алгоритмов симметричного шифрования (ECB, CBC, CFB, OFB).
2. Цифровые водяные знаки.

Преподаватель _____ А.Ю. Иванков

Описание технологии проведения

Для оценивания результатов обучения на зачете 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 (алгоритмов, методик) с использованием математических выкладок, блок-схем, структурных схем и стандартных описаний к ним;
3. умение обосновывать свои суждения и профессиональную позицию по излагаемому вопросу;
4. владение навыками программирования и исследования криптографических алгоритмов обработки информации в рамках выполняемых лабораторных заданий;

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

- 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.

Требования к выполнению заданий, шкалы и критерии оценивания

Критерии оценивания компетенций и шкала оценок (экзамен)

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 лабораторные 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 лабораторные 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 лабораторные 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 лабораторные работы в соответствии с установленным перечнем.	–	Неудовлетворительно