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

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

М.03.03 Информационная безопасность

1. Код и наименование направления подготовки/специальности:

33.08.02 Управление и экономика фармации

2. Профиль подготовки/специализация:

-

3. Квалификация (степень) выпускника:

Провизор - менеджер

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:

05.03.2024, протокол № 5

8. Учебный год:

2025-2026

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 программ и данных, овладение практическими навыками применения методов криптографии, 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 защищенных каналов передачи информации, принципам защиты авторских прав на объекты цифровой интеллектуальной собственности;

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

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

10. Место учебной дисциплины в структуре ООП:

базовый блок дисциплины в общепрофессиональной части. Для успешного освоения дисциплины необходимы входные знания в области математик, информатики, теории информации.

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
ПК-4 готовность к применению основных принципов управления в профессиональной сфере	ПК-4 готовность к применению основных принципов управления в профессиональной сфере	Знает основные теоретические и практические аспекты обеспечения информационной безопасности, основные требования к обеспечению информационной безопасности при обработке конфиденциальной информации, в том числе персональных данных, больничных листов, историй болезни и т.д. Умеет применять на практике теоретические знания в области защиты информации, в том числе современные криптографические средства защиты информации. Владеет практическими навыками применения в профессиональной деятельности специализированных программных средств для обеспечения информационной безопасности.

12. Объем дисциплины в зачетных единицах/час:

2/72

Форма промежуточной аттестации:

Зачет

13. Трудоемкость по видам учебной работы

Вид учебной работы	Семестр 3	Всего
Аудиторные занятия	36	36
Лекционные занятия	0	0
Практические занятия	32	32
Лабораторные занятия	0	0
Контроль самостоятельной работы	2	2
Индивидуальные консультации	2	2
Самостоятельная работа	36	36
Курсовая работа	0	0
Промежуточная аттестация	0	0
Часы на контроль	0	0
Всего	72	72

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК*
1. Практические занятия			
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
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
1.3	Методы и модели оценки уязвимости информации	Эмпирический подход к оценке уязвимости информации.	Создан электронный курс
1.4	Рекомендации по использованию моделей оценки уязвимости информации	Рекомендации по использованию моделей оценки уязвимости информации	Создан электронный курс
1.5	Методы определения требований к защите информации	Методы определения требований к защите информации	Создан электронный курс
1.6	Функции и задачи защиты информации	Общие положения. Методы формирования функций защиты. Классы задач защиты	Создан электронный

		информации. Функции защиты. Состояния и функции системы защиты информации	курс
1.7	Стратегии защиты информации	Стратегии защиты информации.	Создан электронный курс
1.8	Способы и средства защиты информации	Способы и средства защиты информации.	Создан электронный курс
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
1.10	Архитектура систем защиты информации	Требования к архитектуре СЗИ. Построение СЗИ. Ядро системы защиты информации. Ресурсы системы защиты информации.	Создан электронный курс

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (количество часов)				
		Практические	КСР	ИКонс	Самостоятельная работа	Всего
1	Основы государственной информационной политики и информационной безопасности Российской Федерации	2			2	4
2	Информационная безопасность автоматизированных систем	2			2	4
3	Методы и модели оценки уязвимости информации	2			2	4
4	Рекомендации по использованию моделей оценки уязвимости информации	2			2	4
5	Методы определения требований к защите информации	2			2	4
6	Функции и задачи защиты информации	2			2	4
7	Стратегии защиты информации	2			2	4
8	Способы и средства защиты информации	6			8	14

9	Криптографические методы защиты информации	8	2	2	8	20
10	Архитектура систем защиты информации	4			4	8
	Итого:	32	2	2	36	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 практических работ. Подборка вопросов для тестирования осуществляется на основе изученного теоретического материала. Такой подход позволяет повысить мотивацию студентов при конспектировании лекционного материала.

3) 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	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 информати-ка"] / Е.К. Баранова, А.В. Бабаш .— 4-е изд. перераб. и доп. — Москва : РИОР : ИНФРА-М, 2019 .— 334, [1] с. : ил., табл. — (Высшее образование)

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	Рябко, Борис Яковлевич. 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.

№ 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 : Издательскополиграфический центр Воронежского государственного университета, 2013 .— Загл. с титула экрана .— Свободный доступ из интрасети ВГУ .— Текстовый файл .— Windows 2000; Adobe Acrobat Reader .— .
4	Чмора А.Л. Современная прикладная криптография (учебное пособие для ВУЗов) / А.Л. Чмора. – М.: Гелиос АРВ, 2002 – 244с.
5	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 Лань – Лицензионный договор №3010-14/37-23 от 07.03.2023 (срок предоставления с 12.03.2023 по 11.03.2024)
4	ЭБС «Университетская библиотека online»
5	ЭБС «Консультант студента» – Лицензионный договор №3010-06/22-22 от 30.12.2022 (с дополнительным соглашение №1 от 09.01.2023) (срок предоставления с 12.01.2023 по 11.01.2024)

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Основы информационной безопасности [Электронный ресурс] : учеб. пособие / Е.Б. Бе-лов, 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 используется: ПО ОС Windows v.7, 8, 10.
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) 394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, ауд. 479

Учебная аудитория: специализированная мебель, компьютер преподавателя i5-8400-2,8ГГц, монитор с ЖК 19’’, мультимедийный проектор, экран

ПО: ОС Windows v.7, 8, 10, Visual Studio, v. 2010-2019, Набор утилит (архиваторы, файл-менеджеры).

2) 394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, аудитория 292

Учебная аудитория: специализированная мебель, компьютер преподавателя Pentium-G3420-3,2ГГц, монитор с ЖК 17", мультимедийный проектор, экран. Система для ви-деоконференций Logitech ConferenceCam Group и ноутбук 15.6’’ FHD Lenovo V155-15API

ПО: ОС Windows v.7, 8, 10, Visual Studio, v. 2010-2019, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader.

3) 394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, ауд. 380

Учебная аудитория: специализированная мебель, компьютер преподавателя i3-3240-3,4ГГц, монитор с ЖК 17’’, мультимедийный проектор, экран

ПО: ОС Windows v.7, 8, 10, Visual Studio, v. 2010-2019, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader.

4) 394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, аудитория 290

Учебная аудитория: специализированная мебель, персональные компьютеры на базе i7-7800x-4ГГц, мониторы ЖК 27’’ (12 шт.), мультимедийный проектор, экран.

Лабораторное оборудование искусственного интеллекта: рабочие места – персональ-ные компьютеры на базе i7-7800x-4ГГц, мониторы ЖК 27" (12 шт.); модули АО НПЦ «ЭЛ-ВИС»: процессорный Салют-ЭЛ24ПМ2 (9 шт.), отладочный Салют-ЭЛ24ОМ1 (9 шт.), эму-лятор MC-USB-JTAG (9 шт.).

Лабораторное оборудование электроники, электротехники и схемотехники: рабочие ме-ста – персональные компьютеры на базе i7-7800x-4ГГц, мониторы ЖК 27" (12 шт.); стенд для практических занятий по электрическим цепям (KL-100); стенд для изучения анало-говых электрических схем (KL-200); стенд для изучения цифровых схем (KL-300).

ПО: ОС Windows v.7, 8, 10, Visual Studio, v. 2010-2019, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader.

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 1-10	ПК-4	ПК-4	Практические работы 1-6. Тест по соответствующим разделам

Промежуточная аттестация

Форма контроля - зачет

Оценочные средства для промежуточной аттестации

Перечень вопросов, практическое задание

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

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	2	3	4
1	Устный опрос	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 таблице, приведенной ниже

3	Практическая работа	Содержит 4 заданий	При успешном выполнении работы ставится оценка зачтено, в противном случае ставится оценка не зачтено
4	КИМ промежуточной аттестации	Каждый контрольно-измерительный материал для проведения промежуточной аттестации включает 2 заданий вопросов для контроля знаний, умений и владений в рамках оценки уровня сформированности компетенции.	Шкала оценивания приведена ниже

Пример задания для выполнения практической работы

Практическая работа № 1

«Анализ источников, каналов распространения и каналов утечки информации»

Цель работы:

формирование навыка работы с нормативными документами поисследуемому вопросу; анализ угроз информационной безопасности.

Форма контроля: отчет в электронном виде

Количество отведенных аудиторных часов: 1

Задание:

Необходимо провести анализ защищенности объекта защиты информации по следующим разделам:

1. Виды возможных угроз
2. Характер происхождения угроз
3. Классы каналов несанкционированного получения информации
4. Источники появления угроз
5. Причины нарушения целостности информации
6. Потенциально возможные злоумышленные действия
7. Класс защищенности автоматизированной системы

Составить отчёт о проделанной работе, в котором отразить следующие пункты:

1. ФИО исполнителя и номер группы.
2. Название и цель практической работы.
3. Последовательность выполнения работы.
4. Ответы на контрольные вопросы.
5. Выводы.

Примеры контрольных вопросов:

Что такое информационный риск?

Какие существуют методики оценки рисков и управления ими?

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

Приведённые ниже задания рекомендуется использовать при проведении диагностических работ для оценки остаточных знаний по дисциплине.

Задания закрытого типа

1. Защита информации – это

а) деятельность по противодействию случайным угрозам;

б) преднамеренное состояние защищенности объекта;

в) деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию

2. Уголовная ответственность за преступления в информационной сфере предусмотрена в соответствии с какой главой УК РФ:

а) 28;

б) 13

3. Основные задачи информационной безопасности (несколько вариантов):

а) обеспечение целостности;

б) обеспечение конфиденциальности;

в) обеспечение неотслеживаемости;

г) обеспечение доступности;

4. Атрибутами шифра являются:

а) код;

б) алгоритм и ключ;

в) математическая модель

5. Совокупность законов, правил, практических рекомендаций и практического опыта, определяющих управленческие и проектные решения в области защиты информации

а) политика информационной безопасности;

б) положение о защите информации

6. Утечка информации это:

а) несанкционированный процесс переноса информации от источника к злоумышленнику;

б) умышленная передача информации постороннему лицу

7. Моделирование угроз безопасности информации предусматривает:

а) анализ способов ее хищения, изменения и уничтожения с целью оценки наносимого этими способами ущерба;

б) разработка плана мероприятий, направленных на предотвращение и пресечение противоправных действий нарушителя

8. Каким из способов можно определить ценность (стоимость) конфиденциальной информации?

а) прогнозирование возможных штрафов от разглашения, удаления, изменения конфиденциальной информации;

б) прогнозирование стоимости восстановления ресурсов;

в) и способом (а) и способом (б)

9. Предметом криптоанализа являются методы

а) имитозащиты сообщений;

б) шифрования данных;

в) вскрытия шифров

10. Наука об обеспечении конфиденциальности и/или аутентичности передаваемой информации:

а) стеганография;

б) криптография;

в) криптоанализ

11. Целостность – это

а) невозможность несанкционированного просмотра информации;

б) невозможность несанкционированного доступа к информации;

в) невозможность несанкционированного изменения информации

12. В случае применения асимметричной криптосистемы отправитель сообщения использует для шифрования:

а) свой открытый ключ;

б) свой секретный ключ;

в) открытый ключ получателя;

г) секретный ключ получателя

13. Установление санкционированным получателем того факта, что полученное сообщение послано санкционированным отправителем

а) идентификация;

б) авторизация;

в) аутентификация;

г) контроль целостности

14. Под угрозой информационной безопасности понимают:

а) потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам;

б) последствия наступления неблагоприятных событий

15. Электронная подпись – это

а) информация, необходимая для шифрования и расшифровки сообщений;

б) способ преобразования исходного секретного сообщения с целью его защиты;

в) присоединяемый к сообщению блок данных, полученный с использованием криптографического преобразования

16. Каналы несанкционированного доступа

а) через человека;

б) через аппаратуру;

в) через программу;

г) все перечисленные;

17. Ситуация, в которой при использовании различных ключей для шифрования одного и того же сообщения в результате получается один и тот же шифротекст

а) коллизия;

б) избыточность;

в) хеширование

18. Функция, для которой легко найти прямое отображение и очень сложно найти обратное

а) нелинейная;

б) односторонняя;

в) линейная;

г) многозначная

19. Алгоритм Диффи-Хеллмана дает возможность

а) безопасно обменяться общим секретом при условии аутентификации сторон;

б) безопасно обменяться общим секретом;

в) зашифровать сообщение;

г) подписать сообщение

20. Как называют в криптографии называется информация, необходимая для беспрепятственного шифрования и расшифрования сообщений?

а) алгоритм шифрования;

2) ключ;

3) цифровая подпись

21. Функция, предназначенная для сжатия строки произвольной длины до нескольких десятков или сотен бит

а) ЭЦП;

б) логарифмическая функция;

в) функция Эйлера;

г) хеш-функция

22. Алгоритм Диффи-Хеллмана основан на следующей математической задаче

а) факторизации числа;

б) нахождения простых чисел;

в) дискретного логарифмирования

23. Название криптосистем, в которых ключ шифрования и ключ дешифрования совпадают

а) симметричные;

б) асимметричные

24. Наука о скрытой передаче информации путем сохранения в тайне самого факта передачи

а) криптография;

б) стенография;

в) криптоанализ

Задания открытого типа

1. Модель, с помощью которой можно решать и обсуждать концепции безопасности – …

2. Любое действие, направленное на нарушение конфиденциальности, целостности и/или доступности информации, а также на нелегальное использование других ресурсов информационной системы – …

3. Перечислите уровни формирования режима информационной безопасности

…

4. Набор криптографических преобразований или алгоритмов, предназначенных для работы в единой технологической цепочке с целью решения определенной задачи защиты информационного процесса – …

5. Событие, в результате которого произошла или могла произойти утрата одного из свойств криптографического ключа, обеспечивающего безопасность криптосистемы – …

6. Порядок использования ключей в асимметричных криптосистемах при шифровании и расшифровании данных.

Шифрование на … ключе,

расшифрование на … ключе.

Задания с развёрнутым ответом

1. Дайте определение электронной подписи. Нарисуйте обобщенную схему подписывания п проверки подписи. Распишите схему электронной подписи на основе алгоритма RSA (с двумя ключевыми парами).

Критерии оценивания	Шкала оценок
Обучающийся приводит полное и безошибочное определение электронной подписи. Корректную схему подписывания и проверки электронной подписи, а также корректную схему электронной подписи на основе алгоритма RSA.	3 балла
Обучающийся приводит полное и безошибочное определение электронной подписи. Приводит схему подписывания и проверки электронной подписи, а также схему электронной подписи на основе алгоритма RSA. Описание может содержать незначительные неточности.	2 балла
Представлено корректное определение электронной подписи. Схема подписывания и проверки электронной подписи может содержать незначительные неточности. Схема электронной подписи на основе алгоритма RSA не приведена или содержит существенные ошибки.	1 балл
Представлено неполное или содержащее грубые ошибки определение электронной подписи. Схема подписывания и проверки электронной подписи отсутствует или имеет существенные ошибки. Схема электронной подписи на основе алгоритма RSA не приведена или содержит существенные ошибки.	0 баллов

20.2 Промежуточная аттестация

Промежуточная аттестация может включать в себя проверку теоретических вопросов. 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, приведенной 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;
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.

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

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

Результаты обучения оцениваются по бинарной шкале – зачтено или не зачтено по результатам тестирования.

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

Критерии оценивания компетенций и шкала оценок

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	Зачтено
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	Зачтено
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	Зачтено
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.	–	Не зачтено

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

__.__.2024

Направление подготовки / специальность 33.08.02 Управление и экономика фармации

Дисциплина М.03.03 Информационная безопасность

Форма обучения Очное

Вид контроля Зачет

Вид аттестации Промежуточная

Контрольно-измерительный материал № 1

1. Угрозы информационной безопасности

2. Криптографические хеш-функции

Преподаватель_____ М.А. Дрюченко