Федеральное государственное бюджетное образовательное учреждение высшего образования
«Омский государственный аграрный университет имени П.А. Столыпина»

Университетский колледж агробизнеса

ООП по специальности 09.02.11 Разработка и управление программным обеспечением

СОГЛАСОВАНО
Руководитель ООП
_____ Е.А. Поединок
«17» июня 2026 г.

УТВЕРЖДАЮ
Директор
_____ А.П. Шевченко
«17» июня 2026 г.

РАБОЧАЯ ПРОГРАММА
дисциплины
ОП.05 Основы информационной безопасности

Выпускающее отделение	Инженерное отделение	
Разработчики РПУД (внутренние и внешние):		Е.Ю. Комиссарова
Внутренние эксперты:		
Заведующая методическим отделом		Г.А. Горелкина
Директор НСХБ		И.М. Демчукова

Омск, 2026

СОДЕРЖАНИЕ

1.ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ 3
2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ 4
3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ 8
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ 9

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.05 Основы информационной безопасности

1.1. Место дисциплины в структуре основной образовательной программы:

Учебная дисциплина ОП.05 Основы информационной безопасности является обязательной частью общепрофессионального цикла ООП в соответствии с ФГОС СПО по специальности 09.02.11 Разработка и управление программным обеспечением.

Особое значение дисциплина имеет при формировании и развитии общих и профессиональных компетенций ОК 01, ОК 06, ПК 1.5, ПК 4.7

1.2. Цель и планируемые результаты освоения дисциплины:

В рамках программы учебной дисциплины обучающимися осваиваются умения и знания

Код ОК, ПК	Умения	Знания
ОК 01	анализировать задачу и/или проблему и выделять её составные части	основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте
	определять необходимые ресурсы	порядок оценки результатов решения задач профессиональной деятельности
ОК 06	применять стандарты антикоррупционного поведения	стандарты антикоррупционного поведения и последствия его нарушения
ПК 1.5	осуществлять меры по защите компьютерных сетей от несанкционированного доступа	меры защиты информации, реализуемые в автоматизированных (информационных) системах
		методы оценки уязвимости информации
ПК 4.7	использовать и защищать конфиденциальную информацию в процессе ее создания, обработки, передачи	принципы построения организационно-распорядительной системы
		элементы процесса менеджмента ИБ

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем в часах**
Объем образовательной программы учебной дисциплины	80
в т.ч. в форме практической подготовки	-
в т. ч.:	
теоретическое обучение	40
практические занятия	40
Промежуточная аттестация - дифференцированный зачет	

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем, акад. ч / в том числе в форме практической подготовки, акад ч	Коды компетенций и личностных результатов, формированию которых способствует элемент программы	Код Н/У/З
1	2	3	4	5
Раздел 1. Основы информационной безопасности		24/12		
Тема 1.1 Введение в информационную безопасность	**Содержание**	12/6		
	1. Основные понятия и определения информационной безопасности (ИБ). Цели, задачи и принципы обеспечения ИБ.	2	ОК 01, ОК 06, ПК 1.5, ПК 4.7	уо 01.01 уо 01.01 зо 01.01 зо 01.02 зо 06.01 уо 06.01 у 1.5.01 з 1.5.01 з 1.5.02 у 4.7.01 з 4.7.01 з 4.7.02
	2. Практическая работа №1 Анализ законодательства в области защиты информации и персональных данных.	2		
	3. Модели информационной безопасности. Базовая модель угроз.	2		
	4. Практическая работа №2 Определение объектов защиты на типовом объекте информатизации.	2		
	5. Практическая работа №3 Построение модели угроз для автоматизированной системы.	2		
	6. Информационная безопасность в профессиональной деятельности разработчика ПО.	2		

Тема 1.2 Угрозы и уязвимости	Содержание	12/6		
	7. Классификация угроз информационной безопасности: внешние и внутренние, умышленные и непреднамеренные.	2	ОК 01, ПК 1.5, ПК 4.7	уо 01.01 уо 01.01 зо 01.01 зо 01.02 у 1.5.01 з 1.5.01 з 1.5.02 у 4.7.01 з 4.7.01 з 4.7.02
	8. Основные типы уязвимостей: аппаратные, программные, организационные, человеческие.	2		
	9. Практическая работа №4 Определение угроз объекта информатизации и их классификация.	2		
	10. Практическая работа №5 Идентификация и анализ уязвимостей в типовой информационной системе.	2		
	11. Практическая работа №6 Оценка уровня защищенности информационных ресурсов предприятия.	2		
	12. Основные виды атак и вредоносного программного обеспечения. Методы противодействия.	2		
Раздел 2. Методы и средства защиты информации		28/14		
Тема 2.1 Криптографические методы защиты	Содержание	10/6		
	13. Основы криптографии: понятие шифрования, дешифрования, ключа. Симметричное и асимметричное шифрование.	2	ПК 1.5, ПК 4.7	у 1.5.01 з 1.5.01 з 1.5.02 у 4.7.01 з 4.7.01 з 4.7.02
	14. Алгоритмы и протоколы шифрования. Электронная подпись и сертификаты.	2		
	15. Практическая работа №7 Изучение работы алгоритмов шифрования (симметричных и асимметричных).	2		

	16. Практическая работа №8 Применение криптографических средств для защиты файлов и сообщений.	2		
	17. Практическая работа №9 Настройка и использование электронной подписи.	2		
Тема 2.2 Организационно-технические средства защиты	Содержание	16/6		
	18. Антивирусная защита: классификация, принципы работы, современные решения.	2	ПК 1.5, ПК 4.7	у 1.5.01 з 1.5.01 з 1.5.02 у 4.7.01 з 4.7.01 з 4.7.02
	19. Сетевые средства защиты: межсетевые экраны, системы обнаружения вторжений, VPN.	2		
	20. Практическая работа №10 Конфигурирование базовых правил межсетевого экрана.	2		
	21. Управление доступом и идентификация пользователей: парольные политики, биометрия, двухфакторная аутентификация.	2		
	22. Практическая работа №11 Разработка политики паролей и системы контроля доступа.	2		
	23. Резервное копирование и восстановление данных как элемент обеспечения информационной безопасности.	2		
	24. Практическая работа №12 Планирование и реализация стратегии резервного копирования.	2		
	25. Защита персональных данных: требования, меры, ответственность.	2		
Раздел 3. Управление информационной безопасностью		30/14		

Тема 3.1 Организация системы защиты информации	Содержание	14/6	ПК 1.5, ПК 4.7	у 1.5.01 з 1.5.01 з 1.5.02 у 4.7.01 з 4.7.01 з 4.7.02
	26. Построение системы информационной безопасности предприятия: политика, процедуры, регламенты.	2		
	27. Роли и обязанности в области ИБ. Ответственные лица и службы безопасности.	2		
	28. Практическая работа №13 Разработка фрагмента политики информационной безопасности.	2		
	29. Практическая работа №14 Составление инструкции по безопасной работе с информацией для сотрудников.	2		
	30. Инциденты информационной безопасности: классификация, процедуры реагирования.	2		
	31. Практическая работа №15 Разработка плана реагирования на инциденты информационной безопасности.	2		
	32. Практическая работа №16 Выбор мер защиты информации для автоматизированного рабочего места	2		
Тема 3.2 Стандарты и сертификация в области ИБ	Содержание	16/8		
	33. Международные и национальные стандарты ИБ: ISO/IEC 27000, ГОСТ Р ИСО/МЭК 27001.	2	ПК 1.5, ПК 4.7	у 1.5.01 з 1.5.01 з 1.5.02 у 4.7.01 з 4.7.01 з 4.7.02
	34. Системы и схемы сертификации в области информационной безопасности.	2		
	35. Практическая работа №17 Сравнительный анализ требований стандартов ИБ.	2		

	36. Практическая работа №18 Разработка требований к системе защиты информации в соответствии со стандартами.	2		
	37. Документирование процессов в области ИБ: акты, протоколы, отчеты.	2		
	38. Практическая работа №19 Составление отчета о проведении аудита информационной безопасности.	2		
	39. Обеспечение безопасности на всех этапах жизненного цикла программного продукта.	2		
	40. Практическая работа №20 Разработка плана мероприятий по обеспечению безопасности разрабатываемого ПО.	2		
Всего:		80		

3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Для реализации программы учебной дисциплины должны быть предусмотрены следующие специальные помещения:

Кабинет, оснащенный в соответствии с п. 6.1.2 образовательной программы по специальности 09.02.11 Разработка и управление программным обеспечением.

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации укомплектован печатными и/или электронными образовательными и информационными ресурсами, для обеспечения образовательного процесса.

3.2.1. Основные печатные издания

Печатных изданий нет

3.2.2. Основные электронные издания

1. Баранова, Е. К. Основы информационней безопасности : учебник / Е.К. Баранова, А.В. Бабаш. — Москва : РИОР : ИНФРА-М, 2026. — 202 с. — (Среднее профессиональное образование). — DOI: https://doi.org/10.29039/01806-4. - ISBN 978-5-369-01806-4. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2233508 . – Режим доступа: по подписке.

2. Сычев, Ю. Н. Основы информационной безопасности : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2026. — 337 с. — (Среднее профессиональное образование). - ISBN 978-5-16-019432-5. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2221361 . – Режим доступа: по подписке.

3.2.3. Дополнительные источники

1. Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н.В. Гришина. — 2-е изд., доп. — Москва : ИНФРА-М, 2026. — 216 с. — (Среднее профессиональное образование). - ISBN 978-5-16-016719-0. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2242631 . – Режим доступа: по подписке.

2. Редькина, Н. С. Основы информационной культуры и информационной безопасности : учебное пособие / Н.С. Редькина. — Москва : ИНФРА-М, 2025. — 193 с. — (Среднее профессиональное образование). - ISBN 978-5-16-020142-9. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2161237 . – Режим доступа: по подписке.

3. Воройский, Ф. С. Информатика. Новый систематизированный толковый словарь-справочник (Введение в современные информационные и телекоммуникационные технологии в терминах и фактах) / Воройский Ф. С. - 3-е изд. ,перераб. и доп. - Москва: ФИЗМАТЛИТ, 2011. - 760 с. - ISBN 978-5-9221-0426-5. - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL: https://www.studentlibrary.ru/book/ISBN9785922104265.html. - Режим доступа: по подписке.

4. Федеральный закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. N 149-ФЗ, с изменениями и дополнениями: принят Государственной Думой 8 июля 2006 года. – Текст: электронный // Консультант плюс: справочная правовая система. – Москва, 1997. – Загл. с титул.экрана

5. Информационные технологии. – Москва : Новые технологии, 1995. – Выходит ежемесячно. – ISSN 1684-6400. – Текст : электронный. – URL: https://eivis.ru/browse/publication/115066.
6. Современные профессиональные базы данных (ИОСОмГАУ-Moodle).
7. Справочная правовая система КонсультантПлюс.
8. Электронно-библиотечная система издательства «Лань».
9. Электронно-библиотечная система «Znanium.com».
10. Электронно-библиотечная система «Консультант студента».
11. Универсальная База Данных ИВИС (https://eivis.ru/)

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения	***Критерии оценки***	***Методы оценки***
Знания:		
основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте	Обучающийся знает основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте	- устные и письменные опросы на теоретических и практических занятиях; - тестовые опросы; - письменные работы по завершению разделов; - взаимный контроль при работе в парах и малыми группами; - самоконтроль при рефлексии на теоретических занятиях; - наблюдение, интерпретация результатов и экспертная оценка деятельности обучающихся на практических и теоретических занятиях; - итоговый контроль – дифзачет
порядок оценки результатов решения задач профессиональной деятельности	Обучающийся знает порядок оценки результатов решения задач профессиональной деятельности	
стандарты антикоррупционного поведения и последствия его нарушения	Обучающийся знает стандарты антикоррупционного поведения и последствия его нарушения	
меры защиты информации, реализуемые в автоматизированных (информационных) системах	Обучающийся знает меры защиты информации, реализуемые в автоматизированных (информационных) системах	
методы оценки уязвимости информации	Обучающийся знает методы оценки уязвимости информации	
принципы построения организационно-распорядительной системы	Обучающийся знает принципы построения организационно-распорядительной системы	
элементы процесса менеджмента ИБ	Обучающийся знает элементы процесса менеджмента ИБ	
Умения		
анализировать задачу и/или проблему и выделять её составные части	Обучающийся умеет анализировать задачу и/или проблему и выделять её составные части	- проверка результатов и хода выполнения практических работ; - решение поисковых задач; - наблюдение, интерпретация результатов и экспертная оценка
определять необходимые ресурсы	Обучающийся умеет определять необходимые ресурсы	

применять стандарты антикоррупционного поведения	Обучающийся умеет применять стандарты антикоррупционного поведения	деятельности обучающихся на практических и теоретических занятиях; - итоговый контроль – дифзачет
осуществлять меры по защите компьютерных сетей от несанкционированного доступа	Обучающийся умеет осуществлять меры по защите компьютерных сетей от несанкционированного доступа	
использовать и защищать конфиденциальную информацию в процессе ее создания, обработки, передачи	Обучающийся умеет использовать и защищать конфиденциальную информацию в процессе ее создания, обработки, передачи	

Приложение

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Омский государственный аграрный университет имени П.А. Столыпина»

Университетский колледж агробизнеса

09.02.11 Разработка и управление программным обеспечением

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине
ОП 05. Основы информационной безопасности

Обеспечивающее преподавание дисциплины подразделение	Инженерное отделение

Разработчик:

Преподаватель		Т.О.Кортусова

Омск
2026

СОДЕРЖАНИЕ

1.ОБЩИЕ ПОЛОЖЕНИЯ 3

2.ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ ИЗУЧЕНИЯ 4

3.РАСПРЕДЕЛЕНИЕ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ И ТИПОВ ОЦЕНОЧНЫХ МАТЕРИАЛОВ ПО ЭЛЕМЕНТАМ ЗНАНИЙ И УМЕНИЙ 5

4.МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОЦЕНКИ ЗНАНИЙ, УМЕНИЙ 6

5.ПОКАЗАТЕЛИ ОЦЕНКИ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ 10

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Фонд оценочных средств (далее – ФОС) предназначен для контроля и оценки образовательных достижений обучающихся, освоивших программу дисциплины ОП.05 Основы информационной безопасности.
2. ФОС включает оценочные материалы для проведения текущего контроля и промежуточной аттестации в форме дифференцированного зачета.
3. ФОС позволяет оценивать знания, умения, направленные на формирование компетенций.
4. ФОС разработан на основании положений основной образовательной программы по специальности 09.02.11 Разработка и управление программным обеспечением происхождения дисциплины ОП 05. Основы информационной безопасности.
5. ФОС является обязательным обособленным приложением к рабочей программе.

II. ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ ИЗУЧЕНИЯ

Результаты обучения (освоенные умения, усвоенные знания)	Показатели оценки образовательных результатов
ОК 1 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	
анализировать задачу и/или проблему и выделять её составные части	Обучающиеся умеет анализировать задачу и/или проблему и выделять её составные части
определять необходимые ресурсы	Обучающиеся умеет определять необходимые ресурсы
основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте	Обучающийся знает основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте
порядок оценки результатов решения задач профессиональной деятельности	Обучающийся знает порядок оценки результатов решения задач профессиональной деятельности
ОК 6 Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения	
применять стандарты антикоррупционного поведения	Обучающиеся умеет применять стандарты антикоррупционного поведения
стандарты антикоррупционного поведения и последствия его нарушения	Обучающийся знает стандарты антикоррупционного поведения и последствия его нарушения
ПК 1.5 Защищать информацию в базе данных с использованием технологии защиты информации	
осуществлять меры по защите компьютерных сетей от несанкционированного доступа	Обучающиеся умеет осуществлять меры по защите компьютерных сетей от несанкционированного доступа
меры защиты информации, реализуемые в автоматизированных (информационных) системах	Обучающийся знает меры защиты информации, реализуемые в автоматизированных (информационных) системах
методы оценки уязвимости информации	Обучающийся знает методы оценки уязвимости информации
ПК 4.7 Осуществлять защиту данных в мобильных приложения	
использовать и защищать конфиденциальную информацию в процессе ее создания, обработки, передачи	Обучающиеся умеет использовать и защищать конфиденциальную информацию в процессе ее создания, обработки, передачи
принципы построения организационно-распорядительной системы	Обучающийся знает принципы построения организационно-распорядительной системы
элементы процесса менеджмента ИБ	Обучающийся знает элементы процесса менеджмента ИБ

III. РАСПРЕДЕЛЕНИЕ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ И ТИПОВ ОЦЕНОЧНЫХ МАТЕРИАЛОВ ПО ЭЛЕМЕНТАМ ЗНАНИЙ И УМЕНИЙ

Содержание курса	Форма контроля	Знания	Умения
Текущий контроль			
Раздел 1. Основы информационной безопасности			
Тема 1.1 Введение в информационную безопасность	Устный ответ; решение ситуационных задач	зо 01.01 зо 01.02 зо 06.01 з 1.5.01 з 1.5.02 з 4.7.01 з 4.7.02	уо 01.01 уо 01.01 уо 06.01 у 1.5.01 у 4.7.01
Тема 1.2 Угрозы и уязвимости	Устный ответ; решение практических задач	зо 01.01 зо 01.02 з 1.5.01 з 1.5.02 з 4.7.01 з 4.7.02	уо 01.01 уо 01.01 у 1.5.01 у 4.7.01
Раздел 2. Методы и средства защиты информации			
Тема 2.1 Криптографические методы защиты	Устный ответ; решение ситуационных задач	з 1.5.01 з 1.5.02 з 4.7.01 з 4.7.02	у 1.5.01 у 4.7.01
Тема 2.2 Организационно-технические средства защиты	Устный ответ; решение практических задач	з 1.5.01 з 1.5.02 з 4.7.01 з 4.7.02	у 1.5.01 у 4.7.01
Раздел 3. Управление информационной безопасностью			
Тема 3.1 Организация системы защиты информации	Устный ответ; решение задач	з 1.5.01 з 1.5.02 з 4.7.01 з 4.7.02	у 1.5.01 у 4.7.01
Тема 3.2 Стандарты и сертификация в области ИБ	Устный ответ; решение практических задач	з 1.5.01 з 1.5.02 з 4.7.01 з 4.7.02	у 1.5.01 у 4.7.01
Промежуточный контроль			
Дифференцированный зачет	Защита работы	зо 01.01 зо 01.02 зо 06.01 з 1.5.01 з 1.5.02 з 4.7.01 з 4.7.02	уо 01.01 уо 01.01 уо 06.01 у 1.5.01 у 4.7.01

IV. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОЦЕНКИ ЗНАНИЙ, УМЕНИЙ

4.1. Оценочные средства, применяемые для текущего контроля.

Примеры практических (ситуационных) задач

Задание 1.Определить информационный объем пароля (в битах и байтах), если пароль состоит из 8 символов, а алфавит содержит 26 латинских букв (строчные и прописные считаются разными символами) и 10 цифр.

Решение:

Мощность алфавита (N) = 26 (строчные) + 26 (прописные) + 10 (цифры) = 62 символа.
Информационный вес одного символа (i) = $\log_2(62) \approx 5{,}95$ бит. Округляем до 6 бит (так как символ кодируется целым числом бит).
Объем пароля = 8 * 6 = 48 бит = 6 байт.
Ответ: 48 бит (6 байт).

Задание 2.Определить количество возможных комбинаций (стойкость) для 4-значного PIN-кода, состоящего только из цифр, если цифры могут повторяться.

Решение:

Количество символов в алфавите (цифры) = 10.
Длина PIN-кода = 4 символа.
Количество комбинаций = $10^4 = 10\,000$.
Ответ: 10 000 комбинаций.

Задание 3.Рассчитать время полного перебора (брутфорса) пароля длиной 6 символов, состоящего только из цифр, если скорость перебора составляет 1 000 000 паролей в секунду.

Решение:

Количество комбинаций = $10^6 = 1\,000\,000$.
Время = 1 000 000 / 1 000 000 = 1 секунда.
Ответ: ≈ 1 секунда.

Задание 4.Определить энтропию (информационную неопределенность) пароля в битах, если он генерируется из алфавита, содержащего 94 символа (все печатные ASCII-символы), а длина пароля — 10 символов.

Решение:

Энтропия (H) = Длина * $\log_2$(Мощность алфавита).
H = 10 * $\log_2(94) \approx 10 * 6{,}55 = 65{,}5$ бит.
Ответ: ≈ 65,5 бит.

Задание 5.Сколько существует различных паролей длиной 5 символов, если первый символ обязательно должен быть заглавной латинской буквой (26 вариантов), а остальные 4 символа могут быть любыми цифрами (10 вариантов каждый)?

Решение:

Количество вариантов = 26 * 10 * 10 * 10 * 10 = 26 * 10^4 = 260 000.
Ответ: 260 000 комбинаций.

Задание 6.Определить коэффициент сжатия (в процентах) при архивации файла, если исходный размер файла составлял 2 Мбайта, а после сжатия — 512 Кбайт.

Решение:

Переведем в Кбайты: 2 Мбайта = 2 * 1024 = 2048 Кбайт.
Коэффициент сжатия = (Размер_после / Размер_до) * 100% = (512 / 2048) * 100% = 25%.
Размер уменьшился на 100% - 25% = 75%.
Ответ: 25% от исходного (сжатие в 4 раза).

Задание 7.Рассчитать, сколько времени (в днях) потребуется злоумышленнику для подбора 8-символьного пароля, состоящего из строчных латинских букв (26 шт.) и цифр (10 шт.), если скорость перебора составляет 100 000 паролей в секунду, а пароль может начинаться с любого символа.

Решение:

Мощность алфавита = 26 + 10 = 36.
Количество комбинаций = 36^8 = 2 821 109 907 456 (≈ 2,82 * 10^{12}).
Время в секундах = 2 821 109 907 456 / 100 000 = 28 211 099 секунд.
Перевод в дни: 28 211 099 / 86400 ≈ 326,5 дней.
Ответ: ≈ 327 дней (без учета аппаратного ускорения).

Задание 8.Определить, какой объем ключевой информации (в байтах) необходимо распределить между 5 абонентами для организации симметричного шифрования (каждый с каждым должен обменяться секретным ключом), если длина одного ключа — 16 байт.

Решение:

Количество уникальных пар абонентов = C(5,2) = 5! / (2! * 3!) = 10 пар.
Для каждой пары нужен свой ключ.
Общий объем = 10 пар * 16 байт = 160 байт.
Ответ: 160 байт.

Задание 9.Сравнить стойкость (время перебора в секундах) двух паролей при скорости подбора 10^6 паролей/с.
Пароль А: состоит из 6 строчных латинских букв (26 символов).
Пароль Б: состоит из 6 цифр (10 символов).

Решение:

Пароль А: комбинаций = 26^6 = 308 915 776. Время = 308 915 776 / 10^6 ≈ 309 секунд.
Пароль Б: комбинаций = 10^6 = 1 000 000. Время = 1 000 000 / 10^6 = 1 секунда.
Разница: 309 / 1 = 309 раз (Пароль А в 309 раз стойче).
Ответ: Пароль А — ≈ 309 сек, Пароль Б — 1 сек.

Задание 10.Определить максимальную длину пароля (в символах), которую можно гарантированно восстановить за 1 час при скорости подбора 10 000 паролей/с, если пароль состоит только из цифр (10 вариантов на позицию).

Решение:

Максимальное число попыток за час = 10 000 * 3600 = 36 000 000.
Количество комбинаций для длины N = 10^N.
Нужно, чтобы 10^N ≤ 36 000 000.
Проверяем: 10^7 = 10 000 000 (помещается), 10^8 = 100 000 000 (не помещается).
Значит, максимальная длина N = 7.
Ответ: 7 символов.

Примеры тестовых заданий

Компетенции	Оценочные средства
ОК 1 Выбирать способы решения задач профессиональной деятельности применительно к различным	1. **Системы осуществляющие все этапы обработки информации по алгоритму** роботизированные информационно-решающие алгоритмические информационно-управленческие

<table>
<tr>
<td>контекстам</td>
<td>
2. Видеокарты по подключению бывают
УКАЖИТЕ НЕ МЕНЕЕ ДВУХ ВАРИАНТОВ ОТВЕТА
дискретные
твердотельные
интегрированные
игровые

3. Нарушение системы охлаждения приводит к…
снижению скорости передачи данных
перегреву
долгой загрузке
высокому уровню шума

4. Этапы работы приложения:
УКАЖИТЕ ПОРЯДКОВЫЙ НОМЕР ДЛЯ ВСЕХ ВАРИАНТОВ ОТВЕТА
инициализация
запуск
выполнение работы
сохранение и выключение

5. Информационные революции в порядке возрастания:
УКАЖИТЕ ПОРЯДКОВЫЙ НОМЕР ДЛЯ ВСЕХ ВАРИАНТОВ ОТВЕТА
Изобретение письменности
Изобретение книгопечатания
Изобретение средств связи
Изобретение микропроцессора

6. Известны следующие данные о объеме информации.
<table>
<tr><td>Личные данные</td><td>1024 Мб</td></tr>
<tr><td>Рабочие файлы</td><td>2048 Мб</td></tr>
<tr><td>Драйвера</td><td>512 Мб</td></tr>
<tr><td>Временные файлы</td><td>256 Мб</td></tr>
<tr><td>Скрытые файлы</td><td>256 Мб</td></tr>
</table>
7. Общий объем информации в гигабайтах составит...
ВВЕДИТЕ В ПОЛЕ ЧИСЛОВОЕ ЗНАЧЕНИЕ

8. Группировка информации по тематике в поисковых системах представляет собой…
ВВЕДИТЕ В ПОЛЕ СЛОВО В ИМЕНИТЕЛЬНОМ ПАДЕЖЕ

9. Период отказа системы или программы из-за нехватки ресурса называется…
ВВЕДИТЕ В ПОЛЕ СЛОВОСОЧЕТАНИЕ

10. Объем оперативной памяти измеряется в…
ВВЕДИТЕ В ПОЛЕ СЛОВО В ИМЕНИТЕЛЬНОМ ПАДЕЖЕ
</td>
</tr>
<tr>
<td>ОК 6 Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-</td>
<td>
1. К приложениям позволяющим совместно работать над проектами относятся…
github
gantt
clrscr
raviuz

2. Приложения для работы с текстом и графикой…
УКАЖИТЕ НЕ МЕНЕЕ ДВУХ ВАРИАНТОВ ОТВЕТА
</td>
</tr>
</table>

нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения	+ MS Office MSStudio +Libre Office Bitrix 3. **Формат исполняемых файлов …** psd,ppt rar,zip +exe raruz 4. **Укажите соответствие годов появления языка программирования:** 1. C++ — 1. 1985 год 2. Pascal — 2. 1970 год 3.Java — 3. 1996 год. 4. 1962 год 5. **Соответствие видов языков программирования...** 1. Pascal — 1. Структурные 2. PHP — 2. Процедурные 3. Java — 3. Объектно-ориентированные 4. Логические 6. **Уровни репозиториев по уровню увеличения располагаются следующим образом:** УКАЖИТЕ ПОРЯДКОВЫЙ НОМЕР ДЛЯ ВСЕХ ВАРИАНТОВ ОТВЕТА модельный программный репозиторий окружения 7. **Расположите элементы базы данных по увеличению:** УКАЖИТЕ ПОРЯДКОВЫЙ НОМЕР ДЛЯ ВСЕХ ВАРИАНТОВ ОТВЕТА ячейка запись поле таблица 8. **В процессе работы образовался “системный тупик”, укажите значение загрузки RAM.** ВВЕДИТЕ В ПОЛЕ ЧИСЛОВОЕ ЗНАЧЕНИЕ 9. **Известны следующие данные о текущей загрузке RAM на 50%.** Графическое приложение — 2048 мб Аудио приложение — 512 мб Интернет соединение — 512 мб

	<table><tr><td>Процесс скачивания информации</td><td>256 мб</td></tr><tr><td>Прочие процессы</td><td>768 мб</td></tr></table> 10. **Объем носителя информации DVD равен Мб** ВВЕДИТЕ В ПОЛЕ ЧИСЛОВОЕ ЗНАЧЕНИЕ
ПК 1.5 Защищать информацию в базе данных с использованием технологии защиты информации	**1. Автоматизация систем поиска бывает** УКАЖИТЕ НЕ МЕНЕЕ ДВУХ ВАРИАНТОВ ОТВЕТА ручные удаленные автоматизированные примитивные **2. Системы выполняющие все этапы обработки информации по определенному алгоритму** роботизированные информационно-решающие алгоритмические информационно-управленческие **3. Переход на необходимую информацию в глобальной или локальной сети помогают осуществить** УКАЖИТЕ НЕ МЕНЕЕ ДВУХ ВАРИАНТОВ ОТВЕТА поисковые запросы поиск по каталогу гиперссылки удаленный доступ **4. На результат поиска в поисковой системе влияет…** количество символов точность запроса используемая поисковая система скорость интернета **5. Режимы работы поисковых систем…** offline online пакетная передача данных разграниченный доступ **6. Поисковые системы различаются …** УКАЖИТЕ НЕ МЕНЕЕ ДВУХ ВАРИАНТОВ ОТВЕТА механизмом поиска доступностью количеством ответов областью интернета **7. К поисковым системам не относятся…** google amigo yandex yahoo **8. Очередность появление поисковых систем:** УКАЖИТЕ ПОРЯДКОВЫЙ НОМЕР ДЛЯ ВСЕХ ВАРИАНТОВ ОТВЕТА 1. wandex 2. яndex 3. google 4. edge

	9.Абстрактное понятие об расположении компонентов внутри системного блока... ВВЕДИТЕ В ПОЛЕ СЛОВОСОЧЕТАНИЕ. **10. Набор понятий и терминов, характеризующих информационную потребность, и определение отношений между ними.…** ВВЕДИТЕ В ПОЛЕ СЛОВОСОЧЕТАНИЕ
ПК 4.7 Осуществлять защиту данных в мобильных приложения	1. **Требование государственного образца к техническим и программным составляющим …** manual ГОСТ source ISO 2. **Основные виды требований к программному продукту …** УКАЖИТЕ НЕ МЕНЕЕ ДВУХ ВАРИАНТОВ ОТВЕТА функциональные системные пользовательские технические 3. **Этапы создание тестового сценария, протекают в следующей последовательности:** УКАЖИТЕ ПОРЯДКОВЫЙ НОМЕР ДЛЯ ВСЕХ ВАРИАНТОВ ОТВЕТА 1. работа с требованиями. Знакомство с требованиями заказчика 2. разработка стратегии тестирования 3. создание тестовой документации 4. тестирование прототипа 4. **Схема проектирования программных систем в виде последовательности:** УКАЖИТЕ ПОРЯДКОВЫЙ НОМЕР ДЛЯ ВСЕХ ВАРИАНТОВ ОТВЕТА описание требований спецификация проектирование реализация 5. **Локальное видоизменение происходящих в проекте процессов называется** ВВЕДИТЕ В ПОЛЕ СЛОВО В ИМЕНИТЕЛЬНОМ ПАДЕЖЕ 6. **Документ регламентирующий правила и порядок работы в информационных системах называется** ВВЕДИТЕ В ПОЛЕ АББРЕВИАТУРУ 7. **Объем слова ДЕПАРТАМЕНТ в байтах будет равен…** ВВЕДИТЕ В ПОЛЕ ЧИСЛОВОЕ ЗНАЧЕНИЕ 8. **Процесс обнаружения и устранения неисправностей в проекте называется** ВВЕДИТЕ В ПОЛЕ СЛОВО В ИМЕНИТЕЛЬНОМ ПАДЕЖЕ . 9. **К базовым требованиям относятся…** количество разработчиков стоимость название область применения

4.2. Оценочные средства, применяемые для промежуточной аттестации по итогам изучения дисциплины

Дифференцированный зачет проводится по завершении изучения дисциплины на последнем аудиторном занятии.

Промежуточная аттестация по дисциплине в форме дифференцированного зачета осуществляется по результатам текущего контроля успеваемости при выполнении всех видов текущего контроля, предусмотренных рабочей программой дисциплины.

Обучающиеся, не выполнившие виды работ, предусмотренные рабочей программой дисциплины; пропустившие более 50% аудиторных занятий без уважительной причины, не допускаются к дифференцированному зачету.

Промежуточная аттестация таких лиц проводится только после прохождения ими всех видов текущего контроля.

V. ПОКАЗАТЕЛИ ОЦЕНКИ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Уровень сформированности компетенций	**Оценка**	**Критерии оценивания по видам работ**	
		тестирование (процент правильных ответов)	**Прочие виды работ по дисциплине**
Высокий	Отлично	90-100%	Обучающийся глубоко и прочно усвоил теоретический и освоил практический материал. Дает логичные и грамотные ответы. Демонстрирует знание не только основного, но и дополнительного материала, быстро ориентируется, отвечая на дополнительные вопросы. Свободно справляется с поставленными задачами, аргументировано и верно обосновывает Принятые решения.
Повышенный	Хорошо	70-89%	Обучающийся твердо знает программный материал, грамотно и по существу излагает его. Не допускает существенных неточностей при ответах на вопросы, правильно применяет теоретические положения при решении практических задач, владеет навыками и приемами их выполнения.
Базовый	Удовлетворительно	50-69%	Обучающийся демонстрирует знания только основного материала, но не усвоил его детали, испытывает затруднения при решении практических задач. В ответах на поставленные вопросы допускает неточности. Дает определения понятий, неискажающие их смысл. Нарушает последовательность изложения программного материала.
Не сформирована	Неудовлетворительно	0-49%	Обучающийся не знает, не выполняет или неправильно выполняет большую часть учебного материала. Допускает ошибки в формулировке определений, искажающие их смысл, беспорядочно и неуверенно излагает материал. Ответы на дополнительные вопросы отсутствуют. Не выполняет задания.

ЛИСТ РАССМОТРЕНИЙ И ОДОБРЕНИЙ

рабочей программы дисциплины

ОП.05 Основы информационной безопасности

в составе ООП **09.02.11 Разработка и управление программным обеспечением**

1)Рассмотрена и одобрена:
а)На заседании предметно-цикловой методической комиссии протокол № 6 от 10.03.2026 г. Председатель ПЦМК _____С.М. Нурбаева
б) На заседании методического совета протокол №4 от 21.04.2026 г. Председатель методического совета _____М.В. Иваницкая
2)Рассмотрена и одобрена внешним экспертом
а) директор ООО «Сатори Партнер» А.Б. Мальцев