Министерство науки и высшего образования и Российской Федерации

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Комсомольский-на-Амуре государственный университет»

Факультет среднего общего и профессионального образования

УТВЕРЖДАЮ
Декан ФСОиПО
И.В. Конырева

РАБОЧАЯ ПРОГРАММА
учебного предмета **ОП 09 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ**
по специальности среднего профессионального образования
«09.02.01- Компьютерные системы и комплексы»

на базе основного общего образования
Форма обучения очная

Комсомольск-на-Амуре 2025

Рабочая программа учебного предмета **«ОП 09 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ»** составлена на основании Приказа Министерства просвещения Российской Федерации от 25 мая 2022 г. № 362 «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.01 Компьютерные системы и комплексы»

Рабочая программа рассмотрена и одобрена на заседании отделения Среднего профессионального образования – Колледж.

Протокол № 7
от «05» марта 2025 г.

Руководитель отделения СПО-Колледж *Н.Л. Катунцева*

Автор рабочей программы *А.А. Обласов*

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОГО ПРЕДМЕТА «ОП 09 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ»

1.1. Место предмета в структуре основной образовательной программы:

Учебная дисциплина «Информационная безопасность и защита информации» является обязательной частью общепрофессионального цикла примерной основной образовательной программы в соответствии с ФГОС СПО по 09.02.01 Компьютерные системы и комплексы.

Особое значение дисциплина имеет при формировании и развитии **ОК 01.; ОК 02.; ОК 04.; ОК 09.; ПК 1.1.; ПК 1.3.; ПК 2.1.; ПК 3.1.; ПК 3.2.**

1.2. Цель и планируемые результаты освоения учебного предмета

В рамках программы учебной дисциплины обучающимися осваиваются умения и знания

Код ПК, ОК	Умения	Знания
ОК 01.; ОК 02.; ОК 04.; ОК 09.; ПК 1.1.; ПК 1.3.; ПК 2.1.; ПК 3.1.; ПК 3.2.	Уметь: -использовать нормативную правовую базу для решения задач в профессиональной деятельности; - провести анализ защищенности информационной системы. - анализировать и оценивать риски информационной безопасности автоматизированных систем; - реализовывать программные методы защиты информации в автоматизированных системах;	Знать: -теоретические основы защиты информации; - роль информационной безопасности в системе национальной безопасности РФ; - основные виды угроз для информационных систем; - методы и средства защиты информации; - основные принципы построения информационных систем; - стандарты информационной безопасности; - основные законы и стандарты в сфере информационной безопасности; - принципы шифрования и аутентификации пользователей; - принципы работы операционных систем, сетевых протоколов; - основы управления доступом, политики информационной безопасности;

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОГО ПРЕДМЕТА

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем в часах
Объем образовательной программы учебной дисциплины	**110**
в т.ч. в форме практической подготовки	**28**
в т. ч.:	
теоретическое обучение	56
лабораторные работы	28
Самостоятельная работа: в т.ч. подготовка к лабораторным занятиям и тестам	20
консультация	2
экзамен	4
Промежуточная аттестация	7 семестр – экзамен

2.2. Тематический план и содержание учебного предмета «ОП 09 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ»

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем, ак. ч / в том числе в форме практической подготовки, ак. ч	Коды компетенций и личностных результатов[1], формированию которых способствует элемент программы
Раздел 1. Основы информационной безопасности		**12/4**	
Тема 1.1. Теоретические основы ЗИ и ИБ	**Содержание учебного материала**	**6/2**	ОК 01.; ОК 02.; ОК 04.; ОК 09.; ПК 1.1.; ПК 1.3.; ПК 2.1.; ПК 3.1.; ПК 3.2.
	Основные понятия и терминология в сфере информационной безопасности (ИБ).	6	
	Классификация уязвимостей и виды атак на информационные системы. Модели угроз.		
	Законодательные основы защиты информации (ЗИ).		
	В том числе практических и лабораторных занятий	**2**	
	Лабораторное занятие №1 Исследование доктрины информационной безопасности РФ и нормативной, правовой базы в сфере ИБ	2	
	Самостоятельная работа обучающихся: подготовка к тестам	**2**	
Тема 1.2. Современные угрозы информационной безопасности	**Содержание учебного материала**	**6/2**	ОК 01.; ОК 02.; ОК 04.; ОК 09.; ПК 1.1.; ПК 1.3.; ПК 2.1.; ПК 3.1.; ПК 3.2.
	Методы социальной инженерии и защита от фишинга.	6	
	Компьютерные вирусы и вредоносное ПО.		
	Антивирусные программы и технологии предотвращения вторжений.		
	В том числе практических и лабораторных занятий	**2**	
	Лабораторное занятие №2. Изучение принципов работы антивирусных программ и утилит детектирования вредоносного программного обеспечения. Установка и настройка антивируса Kaspersky, Dr.Web или других сертифицированных решений.	2	
	Самостоятельная работа обучающихся: подготовка к тестам	**2**	

[1] В соответствии с Приложением 3 ПООП.

Раздел 2. Криптографическая защита и биометрические системы		**20/10**	
Тема 2.1. Основные криптографической защиты	**Содержание учебного материала**	**8/2**	ОК 01.; ОК 02.; ОК 04.; ОК 09.; ПК 1.1.; ПК 1.3.; ПК 2.1.; ПК 3.1.; ПК 3.2.
	Криптографические методы защиты информации.	8	
	Алгоритмы шифрования и хеширования.		
	Электронная цифровая подпись		
	Управление ключами.		
	В том числе практических и лабораторных занятий	**2**	
	Лабораторное занятие № 3. Изучение инструментов для выявления слабых мест сети и веб-приложений	2	
	Самостоятельная работа обучающихся: подготовка к лабораторным занятиям	**2**	
Тема 2.2. Изучение биометрических систем.	**Содержание учебного материала**	**6/4**	ОК 01.; ОК 02.; ОК 04.; ОК 09.; ПК 1.1.; ПК 1.3.; ПК 2.1.; ПК 3.1.; ПК 3.2.
	Биометрические системы идентификации и аутентификации.	6	
	Обзор современных биометрических решений.		
	Оценка эффективности биометрии.		
	В том числе практических и лабораторных занятий	**4**	
	Лабораторное занятие № 4. Исследование особенностей и возможностей идентификации и аутентификации	4	
	Самостоятельная работа обучающихся: подготовка к лабораторным занятиям	**2**	
Тема 2.3. Безопасность беспроводных сетей	**Содержание учебного материала**	**6/4**	ОК 01.; ОК 02.; ОК 04.; ОК 09.; ПК 1.1.; ПК 1.3.; ПК 2.1.; ПК 3.1.; ПК 3.2.
	Защищенность беспроводных сетей Wi-Fi, Bluetooth и мобильных устройств.	6	
	Средства защиты персональных данных на смартфонах и планшетах.		
	Безопасность IoT-устройств.		
	В том числе практических и лабораторных занятий	**4**	
	Лабораторное занятие № 5. Исследования возможностей межсетевого экранирования	2	
	Лабораторное занятие № 6. Конфигурирование и управление межсетевыми экранами	2	
	Самостоятельная работа обучающихся: подготовка к лабораторным занятиям и тесту по разделу 2	**2**	
Раздел 3. Стандартизация и сертификация в сфере информационной безопасности и защиты информации		**16/6**	
Тема 3.1.	**Содержание учебного материала**	**12/4**	

Стандарты и сертификация информационной безопасности	Международный стандарт ISO/IEC 27001,	12	ОК 01.; ОК 02.; ОК 04.; ОК 09.; ПК 1.1.; ПК 1.3.; ПК 2.1.; ПК 3.1.; ПК 3.2.
	ГОСТ Р 50922		
	Система менеджмента информационной безопасности предприятия.		
	Требования и рекомендации ФСТЭК		
	Требования и рекомендации ФСБ		
	Требования и рекомендации Роскомнадзор		
	В том числе практических и лабораторных занятий	**4**	
	Лабораторное занятие № 7. Методы оценки соответствия требованиям стандартов и контролирующих органов.	4	
	Самостоятельная работа обучающихся: подготовка к лабораторным занятиям	**4**	
Тема 3.2. Особенности обеспечения информационной безопасности облачных сервисов и виртуальных сред	**Содержание учебного материала**	**4/2**	ОК 01.; ОК 02.; ОК 04.; ОК 09.; ПК 1.1.; ПК 1.3.; ПК 2.1.; ПК 3.1.; ПК 3.2.
	Использование облачной инфраструктуры для хранения и обработки конфиденциальной информации.	4	
	В том числе практических и лабораторных занятий	**2**	
	Лабораторное занятие № 8. Исследование возможностей многофакторной аутентификации	2	
	Самостоятельная работа обучающихся: подготовка к лабораторным занятиям и тестам	**2**	
Раздел 4. Обеспечение защиты информации в автоматизированных информационных системах		**8/8**	
Тема 4.1. Методики обеспечения ЗИ в АС	**Содержание учебного материала**	**8/8**	ОК 01.; ОК 02.; ОК 04.; ОК 09.; ПК 1.1.; ПК 1.3.; ПК 2.1.; ПК 3.1.; ПК 3.2.
	Инструменты мониторинга и анализа сетевого трафика	8	
	Стандарты аудита безопасности и реагирования на инциденты.		
	Резервное копирование и восстановление данных		
	Аварийное восстановление и устойчивость ИТ-инфраструктуры.		
	В том числе практических и лабораторных занятий	**8**	
	Лабораторное занятие № 9. Работа с системами обнаружения вторжений	4	
	Лабораторное занятие № 10. Подключение и конфигурирование систем обнаружения вторжений для выявления подозрительной активности в локальной сети.	4	
	Самостоятельная работа обучающихся: подготовка к лабораторным занятиям	**4**	
Консультация		**2**	

Промежуточная аттестация	**4**
	110/28

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОГО ПРЕДМЕТА

3.1. Требования к минимальному материально-техническому обеспечению

Для реализации программы учебной дисциплины должны быть предусмотрены следующие специальные помещения: лаборатория «Прикладного программирования»:

Лаборатория «Прикладного программирования»	Помещение оснащено: специализированная (учебная) мебель (29 компьютерных столов, 30 стульев, доска меловая); оборудование для презентации учебного материала (переносной мультимедийный проектор, экран); технические средства обучения (ПЭВМ Intel Core i3-10100 12 шт. и ПЭВМ Intel Core i3-2330M 16 шт). Оснащенность специальных помещений: выход в интернет, в том числе через wi-fi, обеспечен доступ в электронную информационно-образовательную среду университета. Программное обеспечение: 1 Mathcad Академическое. 2 1С:Предприятие 8.3 (учебная версия) Академическое. 3 7-Zip 16.04 (x64) Свободное. 4 Anylogic Свободное. 5 GNU Octave 3.6.4 Свободное. 6 LocalOff Свободное. 7 Google Chrome Свободное. 8 Kaspersky Security Russian Edition s.

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы, для использования в образовательном процессе. При формировании библиотечного фонда образовательной организацией выбирается не менее одного издания из перечисленных ниже печатных изданий и (или) электронных изданий в качестве основного, при этом список, может быть дополнен новыми изданиями.

3.2.1. Основные печатные издания

1. Баранова, Е. К. Основы информационней безопасности : учебник / Е. К. Баранова, А.В. Бабаш. – Москва : РИОР : ИНФРА-М, 2025. – 202 с. – (Среднее профессиональное образование). – DOI: https://doi.org/10.29039/01806-4. // Znanium : электронно-библиотечная система. – URL: https://znanium.ru./catalog/product/2169040 (дата обращения: 14.03.2025). – Режим доступа: по подписке.

2. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. – 3-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 161 с. – (Профессиональное образование). //

Юрайт : образовательная платформа. – URL: https://urait.ru/bcode/542340 (дата обращения: 14.03.2025). – Режим доступа: по подписке.

3. Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н.В. Гришина. – 2-е изд., доп. – Москва : ИНФРА-М, 2023. – 216 с. – (Среднее профессиональное образование). // Znanium : электронно-библиотечная система. – URL: https://znanium.ru./catalog/product/1900721 (дата обращения: 14.03.2025). – Режим доступа: по подписке.

4. Защита персональных данных : учебное пособие для среднего профессионального образования / О. М. Голембиовская, М. Ю. Рытов, Ю. Ю. Громов [и др.]. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2024. – 156 с. // IPR SMART: цифровой образовательный ресурс. – URL: https://www.iprbookshop.ru/135612.html (дата обращения: 14.03.2025). – Режим доступа: по подписке.

3.2.2. Основные электронные издания

1. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учебное пособие / Ю.Н. Сычев. – 2-е изд., перераб. и доп. – Москва : ИНФРА-М, 2024. – 602 с. – (Среднее профессиональное образование). // Znanium : электронно-библиотечная система. – URL: https://znanium.ru./catalog/product/1942679 (дата обращения: 14.03.2025). – Режим доступа: по подписке.

2. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В. Ф. Шаньгин. – Москва : ФОРУМ : ИНФРА-М, 2024. – 416 с. – (Среднее профессиональное образование). // Znanium : электронно-библиотечная система. – URL: https://znanium.ru./catalog/product/2130242 (дата обращения: 14.03.2025). – Режим доступа: по подписке.

3. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2025. – 252 с. – (Профессиональное образование). // Юрайт : образовательная платформа. – URL: https://urait.ru/bcode/567521 (дата обращения: 14.03.2025). – Режим доступа: по подписке.

3.2.3. Дополнительные источники

1. Ищейнов, В. Я. Основные положения информационной безопасности : учебное пособие / В. Я. Ищейнов, М. В. Мецатунян. – Москва : ФОРУМ : ИНФРА-М, 2024. – 208 с. – (Среднее профессиональное образование). // Znanium : электронно-библиотечная система. – URL:

https://znanium.ru./catalog/product/2138953 (дата обращения: 14.03.2025). – Режим доступа: по подписке.

2. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебник для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. – Москва : Издательство Юрайт, 2025. – 342 с. – (Профессиональное образование). // Юрайт : образовательная платформа. – URL: https://urait.ru/bcode/566079 (дата обращения: 14.03.2025). – Режим доступа: по подписке.

3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. – Москва : Издательство Юрайт, 2025. – 312 с. – (Профессиональное образование). // Юрайт : образовательная платформа. – URL: https://urait.ru/bcode/567283 (дата обращения: 14.03.2025). – Режим доступа: по подписке.

4. Редькина, Н. С. Основы информационной культуры и информационной безопасности : учебное пособие / Н.С. Редькина. – Москва : ИНФРА-М, 2025. – 193 с. – (Среднее профессиональное образование). // Znanium : электронно-библиотечная система. – URL: https://znanium.ru./catalog/product/2161237 (дата обращения: 14.03.2025). – Режим доступа: по подписке.

5. Сычев, Ю. Н. Основы информационной безопасности : учебное пособие / Ю. Н. Сычев. – Москва : ИНФРА-М, 2024. – 337 с. – (Среднее профессиональное образование). // Znanium : электронно-библиотечная система. – URL: https://znanium.ru./catalog/product/2118689 (дата обращения: 14.03.2025). – Режим доступа: по подписке.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОГО ПРЕДМЕТА

Результаты обучения[2]	**Критерии оценки**	**Методы оценки**
Перечень знаний, осваиваемых в рамках дисциплины		
Знать: - понятие и историю развития интеллектуальных систем;	Количество правильных ответов на вопросы теста - не менее 60 %.	Тестирование Экспертное наблюдение и оценивание выполнения лабораторных работ.

- архитектуру и классификацию интеллектуальных систем; - основные понятия машинного обучения; - инструменты и языки для анализа данных; - алгоритмы машинного обучения; - основы нейронных сетей и их практическое применение; - экспертные системы и основы нечёткой логики; - основы обработки естественного языка и генеративные модели; - интеллектуальные системы в компьютерных комплексах	Соответствие результатов работ модельным	
Перечень умений, осваиваемых в рамках дисциплины		
Уметь: -использовать системы искусственного интеллекта для решения задач в профессиональной деятельности; - реализовывать алгоритмы машинного обучения; - работать с библиотеками Python для машинного обучения; - провести оценку качества моделей, полученных с использованием искусственного интеллекта.	Соответствие результатов выполнения и оформления практических заданий модельным результатам и/или примерам выполнения	Экспертное наблюдение и оценивание выполнения практических работ. Текущий контроль в форме защиты лабораторных работ