МИНИСТЕРСТВО ОБРАЗОВАНИЯ РОСТОВСКОЙ ОБЛАСТИ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ РОСТОВСКОЙ ОБЛАСТИ
«РОСТОВСКИЙ-НА-ДОНУ КОЛЛЕДЖ РАДИОЭЛЕКТРОНИКИ, ИНФОРМАЦИОННЫХ И ПРОМЫШЛЕННЫХ ТЕХНОЛОГИЙ»
(ГБПОУ РО «РКРИПТ»)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОП.13 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Специальность:
09.02.13 ИНТЕГРАЦИЯ РЕШЕНИЙ С ПРИМЕНЕНИЕМ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Квалификация выпускника:
специалист по работе с искусственным интеллектом

Форма обучения: очная

Ростов-на-Дону
2026

СОГЛАСОВАНО
И.о. заместителя директора
по учебно-методической работе
_____ М.В. Шевченко
«__» апреля 2026 г.

УТВЕРЖДАЮ
Директор колледжа
_____ Д.В. Лепёшкин
«__» апреля 2026 г.

РАССМОТРЕНО
Цикловой комиссией программирования
компьютерных систем
Протокол № 8 от «20» марта 2026 г.
Председатель ЦК А.Е. Нецветаева

Рабочая программа дисциплины ОП.13 Основы информационной безопасности разработана в соответствии с потребностями рынка труда и запросами работодателей по специальности среднего профессионального образования 09.02.13 Интеграция решений с применением технологий искусственного интеллекта.

Разработчик(и):
Махно Л.В., преподаватель высшей квалификационной категории ГБПОУ РО «РКРИПТ»

Рецензенты:
Полесовая Т.Ю., преподаватель высшей квалификационной категории ГБПОУ РО «РКРИПТ»
Медяников А.А., генеральный директор ООО «Инкост»

СОДЕРЖАНИЕ ПРОГРАММЫ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.13 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Цель и место дисциплины в структуре образовательной программы

Цель дисциплины ОП.13 Основы информационной безопасности: формирование знаний о принципах и методах организации информационной безопасности, освоение умений и навыков выполнения операций по защите данных. Дисциплина ОП.13 Основы информационной безопасности включена в вариативную часть образовательной программы в целях наиболее полного освоения вида деятельности «Администрирование баз данных» и профессиональной компетенции. ПК 2.3. Проводить аудит систем безопасности баз данных с использованием регламентов по защите информации.

1.2. Планируемые результаты освоения дисциплины

Результаты освоения дисциплины соотносятся с планируемыми результатами освоения образовательной программы, представленными в матрице компетенций выпускника.

В результате освоения дисциплины обучающийся должен:

Код ОК, ПК	**Уметь**	**Знать**	**Владеть навыками**
ОК.01	– распознавать задачу и/или проблему в профессиональном и/или социальном контексте, анализировать и выделять её составные части – определять этапы решения задачи, составлять план действия, реализовывать составленный план, определять необходимые ресурсы	– актуальный профессиональный и социальный контекст, в котором приходится работать и жить – структуру плана для решения задач, алгоритмы выполнения работ в профессиональной и смежных областях	-
ОК.02	– определять задачи для поиска информации, планировать процесс поиска, выбирать необходимые источники информации	– номенклатуру информационных источников, применяемых в профессиональной деятельности	-
ОК.05	– грамотно излагать свои мысли и оформлять документы по	– правила оформления документов	-

	профессиональной тематике на государственном языке		
ОК.09	– понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы	– правила построения простых и сложных предложений на профессиональные темы	-
ПК 2.3	- дать независимую оценку уровня безопасности; - производить регламентное обновление программного обеспечения; - разрабатывать перечень рекомендаций по дальнейшей эксплуатации БД с максимальной защитой хранящейся информации.	- протоколы безопасности при работе с базой данных; - методы и средства защиты информации от несанкционированного доступа; - уровни угроз безопасности информации.	- документирования результатов аудита безопасности информации; - использования процедуры резервного копирования баз данных; - использования процедуры восстановления баз данных.

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Трудоемкость освоения дисциплины

Наименование составных частей дисциплины	**Объем в часах**	**В т.ч. в форме практ. подготовки**
Учебные занятия	64	40
Самостоятельная работа	-	-
Промежуточная аттестация в форме экзамена	6	-
Консультации	2	-
Всего	**72**	**40**

2.2. Содержание дисциплины

Наименование разделов и тем	Содержание учебного материала, практических занятий	Объем, ак. ч. / в том числе в форме практической подготовки, ак. ч.	Коды компетенций, формированию которых способствует элемент программы
Тема 1.1. Введение в информационную безопасность	**Содержание**	**2**	ОК.01, ОК.02, ОК.05, ОК.09, ПК 2.3
	Основные понятия и определения. История и развитие информационной безопасности. Актуальные угрозы и риски в информационной безопасности	2	
Тема 1.2. Управление безопасностью информации	**Содержание**	**4**	ОК.01, ОК.02, ОК.05, ОК.09, ПК 2.3
	Нормативно-правовое регулирование в области ИБ. Политики и процедуры безопасности. Оценка рисков и управление ими. Соответствие стандартам и нормативам (ISO 27001, GDPR и др.)	2	
	В том числе практических занятий	**2**	
	Практическое занятие №1. Применение в профессиональной деятельности требований правовых документов государственной политики в сфере информационной безопасности.	2	
Тема 1.3. Криптография	**Содержание**	**6**	ОК.01, ОК.02, ОК.05, ОК.09, ПК 2.3
	Основы криптографии: симметричные и асимметричные алгоритмы. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография.	2	
	В том числе практических занятий	**4**	
	Практическое занятие №2. Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой подписи сообщения.	4/4	
Тема 1.4. Защита сетевой инфраструктуры	**Содержание**	**14**	ОК.01, ОК.02, ОК.05, ОК.09, ПК 2.3
	Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.) Использование VPN и межсетевых экранов. Угрозы при работе в беспроводных сетях. Стандарты из семейства 802.11x. Управление подключениями в точке беспроводного доступа	2	
	В том числе практических занятий	**12**	
	Практическое занятие №3. Организация защиты от атак	4/4	
	Практическое занятие №4. Организация работы VPN и межсетевого экрана	4/4	

	Практическое занятие №5. Настройка защищенного беспроводного соединения	4/4	
Тема 1.5. Безопасность приложений	**Содержание**	**2**	ОК.01, ОК.02, ОК.05, ОК.09, ПК 2.3
	Методы классификации компьютерных вирусов. Анализ программной структуры компьютерных вирусов. Основные методы защиты информации от компьютерных вирусов.	2	
Тема 1.6. Уязвимости веб-приложений	**Содержание**	**8**	ОК.01, ОК.02, ОК.05, ОК.09, ПК 2.3
	Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей.	2	
	В том числе практических занятий	**6**	
	Практическое занятие №6. Тестирование на проникновение и анализ уязвимостей.	2/2	
	Практическое занятие №7. Установка и изучение возможностей антивирусных программ	4/4	
Тема 1.7. Защита данных	**Содержание**	**8**	ОК.01, ОК.02, ОК.05, ОК.09, ПК 2.3
	Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных. Управление доступом к данным	2	
	В том числе практических занятий	**6**	
	Практическое занятие №8. Выполнение резервного копирования и восстановления данных. Управление доступом к данным	4/4	
	Практическое занятие №9. Настройка параметров безопасности. Установка параметров шифрования.	2/2	
Тема 1.8. Безопасность облачных технологий	**Содержание**	**6**	ОК.01, ОК.02, ОК.05, ОК.09, ПК 2.3
	Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности	2	
	В том числе практических занятий	**4**	
	Практическое занятие №10. Изучение модели облачных услуг и их безопасности	4/4	
Тема 1.9. Инциденты безопасности	**Содержание**	**6**	ОК.01, ОК.02, ОК.05, ОК.09, ПК 2.3
	Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента. Кибербезопасность. Промышленный шпионаж. OSINT. Форензика	2	
	В том числе практических занятий	**4**	
	Практическое занятие №11. Работа с инцидентами.	4/4	

Тема 1.10. Социальная инженерия и человеческий фактор	**Содержание**	**6**	ОК.01, ОК.02, ОК.05, ОК.09, ПК 2.3
	Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности	2	
	В том числе практических занятий	**4**	
	Практическое занятие №12. Разработка политики информационной безопасности	4/4	
Тема 1.11. Будущее информационной безопасности	**Содержание**	**2**	ОК.01, ОК.02, ОК.05, ОК.09, ПК 2.3
	Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности	2	
Всего		**64**	
Консультации		**2**	
Экзамен		**6**	
Всего		**72**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение

Кабинет общепрофессиональных дисциплин и профессиональных модулей, оснащённый оборудованием, техническими средствами обучения для проведения занятий всех видов, предусмотренных образовательной программой, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Оборудование и технические средства обучения:

1. Мультимедийное оборудование (мультимедийный проектор, интерактивная доска, клавиатура для лиц с ОВЗ с увел. клавиш, джойстик компьютерный).

2. Программное обеспечение:

- операционная система (Astra Linux Special Edition, Альт Сервер);
- ПО для просмотра документов в формате PDF (Яндекс Браузер);
- ПО для архивации (7-Zip);
- ПО офисный пакет (программный пакет LibreOffice);
- ПО веб-браузер (Яндекс Браузер);
- ПО редактор диаграмм (draw.io);
- ПО Системы контроля версий (Git);
- программная платформа (Anaconda3);
- ПО среда разработки (Microsoft Visual Studio Community);
- среда для разработки графических интерфейсов (Kivy Designer);
- текстовый редактор (Visual Studio Code);
- клиент для работы с API (Postman);
- ПО СУБД (PgAdmin);
- контейнерная платформа (VK Cloud Kubernetes);
- система мониторинга (Zabbix);
- система логирования (LogHouse);
- секрет-менеджер (custom Vault-сервис на базе HashiCorp с Keycloak);
- средства защищённого удалённого доступа (ViPNet Client + OpenVPN или аналоги);
- инструментарий автоматизации развертывания инфраструктуры (Terraform + Ansible);
- решения для автоматизированного контроля уязвимостей (MaxPatrol VM);
- платформа для тестирования на проникновение (КиберПолигон (Ростелеком));
- система документирования инцидентов (АРМ Инцидент, SORM-Трекер);
- облачная среда (Яндекс Облако);
- инструмент бизнес-аналитики и генерации отчётов (СБИС BI).

3. Автоматизированные рабочие места для инвалидов, оборудованные специализированным программным обеспечением, адаптированные для лиц с ограниченными возможностями здоровья, альтернативные устройства ввода информации для обучающихся с нарушениями опорно-двигательного аппарата, звукоусиливающая аппаратура для обучающихся с нарушениями слуха.

4. Автоматизированное рабочее место преподавателя.

Библиотека, читальный зал с выходом в Интернет.

3.2. Учебно-методическое обеспечение

3.2.1. Основные печатные и/или электронные издания

1. Баранова, Е. К. Основы информационной 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 (дата обращения: 22.04.2026).

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 (дата обращения: 22.04.2026).

3. 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 (дата обращения: 22.04.2026).

4. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В.Ф. Шаньгин. — Москва: ИНФРА-М, 2026. — 416 с. — (Среднее профессиональное образование). - ISBN 978-5-16-021164-0. - Текст: электронный. - URL: https://znanium.ru/catalog/product/2207574 (дата обращения: 22.04.2026).

3.2.2. Дополнительные источники

1. Зенков, А. В. Основы информационной безопасности: учебное пособие / А. В. Зенков. - Москва; Вологда: Инфра-Инженерия, 2022. - 104 с. - ISBN 978-5-9729-0864-6. - Текст: электронный. - URL: https://znanium.com/catalog/product/1902587 (дата обращения: 22.04.2026).

2. Баранова, Е. К. Информационная безопасность и защита информации: учебное пособие / Е.К. Баранова, А.В. Бабаш. — 5-е изд., перераб. и доп. — Москва: РИОР: ИНФРА-М, 2026. — 384 с. — (Высшее образование). — DOI: https://doi.org/10.29039/02005-0. - ISBN 978-5-369-02005-0. - Текст: электронный. - URL: https://znanium.ru/catalog/product/2233509 (дата обращения: 22.04.2026).

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Результаты обучения	Показатели освоенности компетенций	Методы оценки
Знает: – актуальный профессиональный и социальный контекст, в котором приходится работать и жить - структуру плана для решения задач, алгоритмы выполнения работ в профессиональной и смежных областях; - номенклатуру информационных источников, применяемых в профессиональной деятельности; правила оформления документов; правила построения простых и сложных предложений на профессиональные темы; - протоколы безопасности при работе с базой данных; - методы и средства защиты информации от несанкционированного доступа; - уровни угроз безопасности информации. *Умеет:* – распознавать задачу и/или проблему в профессиональном и/или социальном контексте, анализировать и выделять её составные части определять этапы решения задачи, составлять план действия, реализовывать составленный план, определять необходимые ресурсы;	Грамотно излагает свои мысли и оформляет документы по соответствующей тематике. Демонстрирует уверенные знания по изученным темам. Проявляет гражданско-патриотическую позицию. Корректно оценивает результаты решения задач. Использует современную научную и профессиональную терминологию.	Экспертная оценка результатов деятельности при выполнении и защите практических работ, тестирования, письменного опроса, фронтального опроса и экзаменационных заданий.

- определять задачи для поиска информации, планировать процесс поиска, выбирать необходимые источники информации; - грамотно излагать свои мысли и оформлять документы по профессиональной тематике на государственном языке; - понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; - дать независимую оценку уровня безопасности; - производить регламентное обновление программного обеспечения; - разрабатывать перечень рекомендаций по дальнейшей эксплуатации БД с максимальной защитой хранящейся информации. <u>Владеет навыками:</u> - документирования результатов аудита безопасности информации; - использования процедуры резервного копирования баз данных; - использования процедуры восстановления баз данных.	Демонстрирует умение эффективно искать информацию, необходимую для решения задачи или проблемы. Демонстрирует уверенное применение полученных знаний в ходе решения (выполнения) практических заданий. Владеет актуальными методами работы в профессиональной и смежных сферах. Обосновывает выводы и суждения. Эффективно взаимодействует в коллективе, в ходе решения задач.	