

Федеральное государственное образовательное бюджетное
учреждение высшего образования
**«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)**

Красноярский филиал Финуниверситета

УТВЕРЖДАЮ
Заместитель директора
по учебно-методической работе
Красноярского филиала
Финуниверситета
В.С. О.С. Вергейчик
«24» июня 2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

по специальности 09.02.11 Разработка и управление программным обеспечением

г. Красноярск – 2026

Рабочая программа дисциплины разработана на основе федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности 09.02.11 Разработка и управление программным обеспечением.

Разработчик:

Россинская Екатерина Вадимовна, преподаватель

(фамилия, имя, отчество, должность, квалификационная категория)

Рабочая программа дисциплины рассмотрена и рекомендована к утверждению на заседании предметной (цикловой) комиссии общепрофессиональных дисциплин.

Протокол от «27» июня 2026 г. № 11

Председатель предметной (цикловой)
комиссии


(подпись)

О.А. Полтавец
(инициалы, фамилия)

1. Общая характеристика рабочей программы дисциплины

1.1. Место дисциплины в структуре основной образовательной программы

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

1.2 Цель и планируемые результаты освоения дисциплины:

В рамках программы дисциплины обучающимися осваиваются умения и знания

Код ОК	Умения	Знания
ОК 01	распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составлять план действия; реализовывать составленный план; определять необходимые ресурсы	актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности
ОК 02	определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач	номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации, современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности
ОК 04	организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности	психологические основы деятельности коллектива, психологические особенности личности
ОК 05	грамотно излагать свои мысли и оформлять документы по профессиональной тематике на государственном языке, проявлять толерантность в рабочем коллективе	правила оформления документов и построения устных сообщений
ПК 1.1	проектировать базы данных	принципы безопасности хранения данных; методы защиты баз данных от внешних угроз

ПК 1.4	администрировать базы данных	стандарты и протоколы безопасности (SSL/TLS, SSH, Kerberos); методы аутентификации и авторизации
ПК 1.5	защищать информацию в базе данных с использованием технологии защиты информации	законодательство и стандарты безопасности (GDPR, HIPAA, PCI DSS); принципы криптографии и методы шифрования данных
ПК 3.1	разрабатывать техническое задание на веб-приложение в соответствии с требованиями заказчика	источники угроз информационной безопасности и меры по их предотвращению; стандарты и протоколы безопасности (HTTPS, OAuth, OpenID Connect)
ПК 3.2	разрабатывать веб-приложения в соответствии с техническим заданием	основные угрозы безопасности мобильных приложений; принципы криптографии и шифрования данных
ПК 3.3	разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием	принципы и методы обеспечения безопасности информационных систем; методы анализа на уязвимости и мониторинга безопасности
ПК 3.5	интегрировать информационную систему с существующими информационными системами заказчика	основы безопасности приложений и инфраструктуры; знание инструментов и технологий для обеспечения безопасности ИТ-инфраструктуры и веб-приложений
ПК 3.7	разрабатывать техническую документацию на эксплуатацию информационной системы	отраслевая нормативная техническая документация; источники информации, необходимой для профессиональной деятельности

2. Структура и содержание дисциплины

2.1. Объем дисциплины и виды учебной работы

Вид учебной работы	Объем в часах
Объем образовательной программы дисциплины	80
Объем работы обучающихся во взаимодействии с преподавателем	48
в том числе:	
теоретическое обучение	24
практические занятия	24
лабораторные занятия	-
контрольные работы	-
самостоятельная работа	14
Консультация	2
Промежуточная аттестация в форме экзамена	16

2.2. Тематический план и содержание дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Коды компетенций, формированию которых способствует элемент программы
1	2	3	4
Раздел 1. Основы информационной безопасности		24	
Тема 1.1 Введение в информационную безопасность	Содержание учебного материала: 1. Основные понятия и определения. История и развитие информационной безопасности. 2. Актуальные угрозы и риски в информационной безопасности.	4 4	ОК 01 ОК 02
Тема 1.2 Управление безопасностью информации	Содержание учебного материала: 1. Нормативно-правовое регулирование в области ИБ. Политики и процедуры безопасности. 2. Оценка рисков и управление ими. Соответствие стандартам (ISO 27001, GDPR).	4 4	ОК 02 ОК 05 ПК 3.7
Тема 1.3 Криптография	Содержание учебного материала: 1. Основы криптографии: симметричные и асимметричные алгоритмы. 2. Хэширование и цифровые подписи. Применение криптографии в приложениях. В том числе практических занятий: 1. Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой подписи сообщения.	6 4 2 2	ОК 01 ПК 1.5 ПК 3.2
Тема 1.4 Защита сетевой информации	Содержание учебного материала: 1. Основы сетевой безопасности. Защита от атак (DDoS, MITM). Использование VPN и межсетевых экранов. В том числе практических занятий: 1. Организация защиты от атак. Организация работы VPN и межсетевого экрана.	6 2 4 4	ОК 01 ОК 04 ПК 3.5
Тема 1.5 Безопасность приложений	Содержание учебного материала: 1. Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. В том числе практических занятий: 1. Тестирование на проникновение и анализ уязвимостей.	6 2 4 4	ОК 01 ПК 3.1 ПК 3.3
Тема 1.6 Защита данных	Содержание учебного материала:	6	

	1. Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных.	2	ПК 1.1 ПК 1.4 ПК 1.5
	В том числе практических занятий:	4	
	1. Выполнение резервного копирования и восстановления данных. Управление доступом к данным.	4	
Раздел 2. Специальные аспекты информационной безопасности		24	
Тема 2.1. Безопасность облачных технологий	Содержание учебного материала:	4	ОК 01 ОК 02
	1. Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасность.	2	
	В том числе практический занятий:	2	
	1. Изучение модели облачных услуг и их безопасности.	2	
Тема 2.2 Инциденты безопасности	Содержание учебного материала:	6	ОК 01 ОК 04 ОК 05
	1. Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика.	4	
	2. Восстановление после инцидента. Кибербезопасность. Промышленный шпионаж. OSINT. Форензика.		
	В том числе практических занятий:	2	
	1. Работа с инцидентами.	2	
Тема 2.3 Социальная инженерия и человеческий фактор	Содержание учебного материала:	4	ОК 01 ОК 04
	Содержание учебного материала:	2	
	1. Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности.		
	В том числе практических занятий	2	
	1. Разработка политики информационной безопасности.	2	
Тема 2.4 Будущее информационно й безопасности	Содержание учебного материала	4	ОК 01 ОК 02
	1. Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). 2. Этические аспекты информационной безопасности.	4	
Консультация		2	
Самостоятельная работа (решение задач по темам, подготовка к практическим занятиям, подготовка к экзамену)		14	
Промежуточная аттестация в форме экзамена		16	
Всего:		80	

3. Условия реализации программы дисциплины

3.1. Материально-техническое обеспечение

Для реализации программы дисциплины предусмотрены следующие специальные помещения (в соответствии с ФГОС СПО и основной образовательной программой СПО):

Учебная аудитория для проведения занятий всех видов, предусмотренных образовательной программой, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации

Кабинет «Информационных технологий»

Мебель:

- посадочные места по количеству обучающихся (столы, стулья);
- рабочее место преподавателя (стол, стул/кресло);
- шкафы для хранения учебных пособий и дидактических материалов.

Оборудование и технические средства:

- доска меловая/маркерная (рекомендуется доска с магнитной поверхностью или интерактивная доска);
- демонстрационный экран;
- мультимедийный проектор;
- компьютер преподавателя с периферией/ноутбук (с лицензионным программным обеспечением, образовательным контентом и системой защиты от вредоносной информации);
- сетевой фильтр.

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации имеет печатные и электронные образовательные и информационные ресурсы для использования в образовательном процессе.

Основные печатные и электронные издания:

1. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебник для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — 2-е изд. — Москва : Издательство Юрайт, 2026. — 352 с. — (Профессиональное образование). — ISBN 978-5-534-19384-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/587457>

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, 2026. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/587458>

Дополнительные источники:

1. Казарин, О. В. Надежность и безопасность программного обеспечения : учебник для вузов / О. В. Казарин, И. Б. Шубинский. — 2-е изд. — Москва :

Издательство Юрайт, 2026. — 352 с. — (Высшее образование). — ISBN 978-5-534-19386-2. — Текст : электронный // Образовательная платформа Юрайт [сайт].

2. Черпаков, И. В. Основы программирования : учебник и практикум для среднего профессионального образования / И. В. Черпаков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 196 с. — (Профессиональное образование). — ISBN 978-5-534-18760-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/561922>.

4. Контроль и оценка результатов освоения дисциплины

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий, устных и письменных опросов, тестировании, а также выполнения обучающимися внеаудиторной самостоятельной работы.

Результаты обучения	Критерии оценки	Методы оценки
Знает: – актуальный профессиональный и социальный контекст; – принципы безопасности хранения данных; – методы защиты баз данных от внешних угроз; – принципы криптографии и методов шифрования данных; – стандарты и протоколы безопасности (SSL/TLS, SSH, Kerberos); – методы аутентификации и авторизации пользователей; – законодательство и стандарты безопасности (GDPR, HIPAA, PCI DSS); – источники угроз информационной безопасности и меры по их предотвращению; – основные угрозы безопасности мобильных приложений; – знание инструментов и технологий для обеспечения безопасности ИТ-инфраструктуры и веб-приложений.	Характеристики демонстрируемых знаний, которые могут быть проверены: – демонстрируется понимание сущности рассматриваемых явлений и процессов; – демонстрируется умение аргументированно анализировать изучаемый материал; – ответы на тестовые задания содержат не менее 90% правильных ответов – оценка «отлично»; – не менее 75% правильных ответов – оценка «хорошо»; – не менее 60% правильных ответов – оценка «удовлетворительно»	Компьютерное тестирование на знание терминологии по теме; Тестирование Контрольная работа Самостоятельная работа.
Умеет: – распознавать задачу и/или проблему в профессиональном и/или социальном контексте; – составлять план	Характеристики демонстрируемых умений: – демонстрируется умение самостоятельно получать результаты выполнения заданий; – демонстрируется умение	Наблюдение за выполнением практического задания. (деятельностью студента) Оценка выполнения

действия; – владеть актуальными методами работы в профессиональной и смежных сферах; – определять задачи для поиска информации; – шифровать данные и обеспечивать их конфиденциальность; – анализ требований безопасности информационных систем; – разрабатывать и реализовывать меры безопасности; – реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию.	устанавливать связи между изучаемыми понятиями.	практического задания (работы)
--	--	---------------------------------------