

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

УТВЕРЖДАЮ
Заместитель директора по
учебной работе

 Н.Ю. Долгова

« 18 » июня 2026г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

по специальности 09.02.11 Разработка и управление программным
обеспечением

Москва 2026 г.

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

Разработчики:

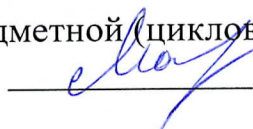
Маринич Анна Леонидовна, преподаватель высшей квалификационной категории

Крымцева Вера Павловна, преподаватель первой квалификационной категории

Рабочая программа дисциплины рассмотрена и рекомендована к утверждению на заседании предметной (цикловой) комиссии
Обеспечение информационной безопасности автоматизированных систем

Протокол от «14» мая 2026 г. №9

Председатель предметной (цикловой)
комиссии



А.Л. Маринич

1. Общая характеристика рабочей программы дисциплины

1.1. Место дисциплины в структуре основной образовательной программы

Учебная дисциплина «ОП.05 Основы информационной безопасности» является обязательной частью цикла образовательной программы в соответствии с ФГОС по специальности 09.02.11 Разработка и управление программным обеспечением.

1.2. Цель и планируемые результаты освоения дисциплины:

В рамках программы дисциплины студентами осваиваются умения и знания

Код общих и профессиональных компетенция	Умения	Знания
ОК.01 ОК.02 ОК.09 ПК 1.1 ПК 1.4 ПК 1.5 ПК 3.1 ПК 3.2 ПК 3.3 ПК 3.5 ПК 3.7	– шифровать данные и обеспечивать их конфиденциальность – анализ требований безопасности информационных систем – разрабатывать и реализовывать меры безопасности – реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию	– принципы безопасности хранения данных – методы защиты баз данных от внешних угроз – принципы криптографии и методов шифрования данных – стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др. – методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных – законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др. – отраслевая нормативная техническая документация – источники информации, необходимой для профессиональной деятельности

Код общих и профессиональных компетенция	Умения	Знания
		– современный отечественный и зарубежный опыт в профессиональной деятельности – принципы и методы обеспечения безопасности информационных систем – принципов безопасности информационных систем – современных методов и технологий в области безопасности информационных систем – законодательных и нормативных актов в области безопасности информационных систем – источники угроз информационной безопасности и меры по их предотвращению – основные угрозы безопасности мобильных приложений – принципы криптографии и шифрования данных. – стандарты и протоколы безопасности, такие как HTTPS, OAuth и OpenID Connect – законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA – основные принципы безопасности информации и методов ее защиты. – стандартные криптографические алгоритмы для шифрования данных – принципы обеспечения безопасности передачи данных по сети – основы безопасности приложений и инфраструктуры

Код общих и профессиональных компетенция	Умения	Знания
		– методы анализа на уязвимости и мониторинга безопасности – знание основных принципов и методов обеспечения безопасности ИТ-инфраструктуры и веб-приложений – понимание различных уязвимостей и угроз безопасности, а также способов их предотвращения и обнаружения – знание инструментов и технологий для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы

2. Структура и содержание дисциплины

2.1. Объем дисциплины и виды учебной работы

Вид учебной работы	Объем в часах
Объем образовательной программы дисциплины	62
Объем работы студентов во взаимодействии с преподавателем	48
в том числе:	
теоретическое обучение	24
практические занятия	24
лабораторные занятия	-
контрольные работы	-
Курсовой проект (работа)(если предусмотрено)	-
самостоятельная работа	2
Промежуточная аттестация в форме экзамена	12

2.2. Тематический план и содержание дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности студентов	Объем в часах	Коды компетенций формированию которых способствует элемент программы.
1	2	3	4
Раздел 1 Основы информационной безопасности		62	
Тема 1.1 Введение в информационную безопасность	Содержание учебного материала	4	ОК.01 ОК.02 ОК.09 ПК 1.1 ПК 1.4 ПК 1.5 ПК 3.1 ПК 3.2 ПК 3.3 ПК 3.5 ПК 3.7
	1. Основные понятия и определения. 2. История и развитие информационной безопасности. 3. Актуальные угрозы и риски в информационной безопасности	2	
	В том числе практических занятий	2	
	1. Практическое занятие «Анализ угроз и защиты в информационной безопасности»	2	
	Самостоятельная работа студентов	-	
Тема 1.2. Управление безопасностью информации	Содержание учебного материала	4	
	1. Нормативно-правовое регулирование в области ИБ. 2. Политики и процедуры безопасности. Оценка рисков и управление ими. 3. Соответствие стандартам и нормативам (ISO 27001, GDPR и др.)	2	
	В том числе практических занятий	2	
	1. Практическое занятие «Оценка рисков ИБ предприятия».	2	
	Самостоятельная работа студентов	-	
Тема 1.3. Криптография	Содержание учебного материала	6	
	1. Основы криптографии: симметричные и асимметричные алгоритмы. 2. Хэширование и цифровые подписи. 3. Применение криптографии в приложениях. Стеганография.	2	
	В том числе практических занятий	4	
	1. Практическое занятие «Работа с	2	

	симметричными и асимметричными алгоритмами» 2. Практическое занятие «Хэширование и создание цифровой подписи сообщения.»	2	
	Самостоятельная работа студентов	-	
Тема 1.4. Защита сетевой инфраструктуры	Содержание учебного материала	8	
	1. Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.) 2. Использование VPN и межсетевых экранов	2	
	В том числе практических занятий	6	
	1. Практическое занятие «Организация защиты от атак» 2. Практическое занятие «Организация работы VPN и межсетевого экрана» 3. <i>Практическое занятие «Расследование сетевой атаки. Обнаружение сканирования портов»*</i>	2 2 2	
	Самостоятельная работа студентов	-	
Тема 1.5. Безопасность приложений	Содержание учебного материала	4	
	1. Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. 2. Тестирование на проникновение и анализ уязвимостей.	2	
	В том числе практических занятий	2	
	Практическое занятие «Тестирование на проникновение и анализ уязвимостей.»	2	
	Самостоятельная работа студентов	-	
Тема 1.6. Защита данных	Содержание учебного материала	4	
	1. Шифрование данных в покое и в транзите. 2. Резервное копирование и восстановление данных. 3. Управление доступом к данным	2	
	В том числе практических занятий	2	
	1. Практическое занятие «Выполнение резервного копирования и восстановления данных.» 2. Практическое занятие «Управление доступом к данным»	2	
	Самостоятельная работа студентов	-	
Тема 1.7. Безопасность облачных	Содержание учебного материала	4	
	Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS,	2	

технологий	SaaS) и их безопасности		
	В том числе практических занятий	2	
	Практическое занятие «Изучение модели облачных услуг и их безопасности»	2	
	Самостоятельная работа студентов	-	
Тема 1.8. Инциденты безопасности	Содержание учебного материала	6	
	1. Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента. 2. Кибербезопасность. Промышленный шпионаж. OSINT. Форензика 3. <i>Защита личных и корпоративных данных от киберугроз*</i>	4	
	В том числе практических занятий	2	
	Практическое занятие «Работа с инцидентами.»	2	
	Самостоятельная работа студентов	-	
Тема 1.9. Социальная инженерия и человеческий фактор	Содержание учебного материала	4	
	Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности <i>Обнаружение фишинга и приемов социальной инженерии*</i>	2	
	В том числе практических занятий	2	
	Практическое занятие «Разработка политики информационной безопасности.»	2	
	Самостоятельная работа студентов Эссе, примерная тематика: 1. Социальная инженерия в соцсетях: как публичная информация становится оружием. 2. Почему умные люди попадают на фишинг? 3. Человеческий фактор внутри компании: почему принесенная флешка опаснее хакера? 4. Классические и современные методы фишинга 5. Как социальная инженерия заставляет честных людей нарушать правила	2	
Тема 1.10. Будущее информационной безопасности	Содержание учебного материала	4	
	Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности <i>Квантовые системы шифрования*</i>	4	
	В том числе практических занятий	-	
	Самостоятельная работа студентов	-	

Промежуточная аттестация в форме экзамена	12	
Всего:	62	

4. Условия реализации дисциплины

3.1. Для реализации программы дисциплины должны быть предусмотрены следующие специальные помещения: в соответствии с ФГОС СПО и ПООП: Лаборатория «Компьютерных сетей и основ информационной безопасности»,

- автоматизированные рабочие места обучающихся (Моноблок – Intel Core i5, RAM 16 Gb, 1 Tb), АРМ подключены к локальной вычислительной сети Интернет;
- автоматизированное рабочее место преподавателя (Моноблок – Intel Core i5, RAM 16 Gb, 1 Tb), АРМ подключен к локальной вычислительной сети Интернет;
- комплексы компьютерных комплектующих для производства сборки, разборки и сервисного обслуживания ПК и оргтехники;
- проектор и экран;
- меловая доска;
- программное обеспечение общего и профессионального назначения, в том числе включающее в себя следующее ПО:

Postman, OBS Studio, VirtualBox, Node.js, Microsoft Visual Studio, Visual Studio Code, Google Chrome, Firefox, Git, Gogs, Notepad++.

3.2. Информационное обеспечение реализации программы

Основные печатные и электронные издания:

1. Баланов, А. Н. Защита информационных систем. Кибербезопасность : учебное пособие для спо / А. Н. Баланов. – 3-е изд., стер.— Санкт-Петербург : Лань, 2026. — 84 с. — ISBN 978-5-507-55006-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://reader.lanbook.com/book/515089#2> (дата обращения: 16.11.2024).

2. Баланов, А. Н. Комплексная информационная безопасность : учебное пособие для спо / А. Н. Баланов. — 2-е изд., стер.--Санкт-Петербург : Лань, 2025. — 284 с. — ISBN 978-5-507-52593-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://reader.lanbook.com/book/463001#2> (дата обращения: 16.11.2024).

3. Нестеров, С. А. Основы информационной безопасности : учебник для спо / С. А. Нестеров. — 3-е изд., стер. — Санкт-Петербург : Лань, 2026. — 324 с. — ISBN 978-5-507-56692-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://reader.lanbook.com/book/518575#2> (дата обращения: 16.11.2024)

4. Прохорова, О. В. Информационная безопасность и защита информации : учебник для спо / О. В. Прохорова. — 7-е изд., стер. — Санкт-Петербург : Лань, 2026. — 124 с. — ISBN 978-5-507-56325-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://reader.lanbook.com/book/515187#2> (дата обращения: 16.11.2024)

4. Контроль и оценка результатов освоения дисциплины

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий, тестирования, а также выполнения студентами индивидуальных заданий, проектов, исследований.

Результаты обучения	Критерии оценки	Методы оценки
Знает: - 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 - номенклатуру информационных источников, применяемых в профессиональной деятельности; - приемы структурирования информации; - формат оформления результатов поиска информации, современные средства и устройства информатизации; - порядок применения современных средств и устройств информатизации и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств; - лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; - принципы безопасности хранения	5 (Отлично) Ориентируется в профессиональном и социальном контексте, в котором приходится работать и жить Владеет основными источниками информации и ресурсами для решения задач в профессиональном и/или социальном контексте Может произвести оценку результатов решения задач профессиональной деятельности Владеет номенклатурой информационных источников, применяемых в профессиональной деятельности Знает формат оформления результатов поиска информации, современные средства и устройства информатизации Может применять современные средства и устройства информатизации и программное обеспечение (в т.ч. цифровые средства) Владеет методами защиты баз данных от внешних угроз Ориентируется в стандартах и протоколах безопасности (SSL/TLS, SSH, Kerberos и др.) Знает методы аутентификации и	Экспертное наблюдение выполнения практических работ и видов работ по практике Диагностика (тестирование) Экзамен

данных; - методы защиты баз данных от внешних угроз - принципы криптографии и методов шифрования данных; - стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др.; - методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.; - отраслевую нормативную техническую документацию и источники информации, необходимые для профессиональной деятельности; - современный отечественный и зарубежный опыт в профессиональной деятельности; - принципы и методы обеспечения безопасности информационных систем; - принципы безопасности информационных систем; - современные методы и технологии в области безопасности информационных систем; - законодательные и нормативные акты в области безопасности информационных систем; - источники угроз информационной безопасности и меры по их предотвращению; - основные угрозы безопасности мобильных приложений; - принципы криптографии и шифрования данных; - стандарты и протоколы безопасности, такие как HTTPS, OAuth и OpenID Connect; - законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA;	авторизации (пароли, сертификаты, биометрия) Знает законодательство и стандарты безопасности (GDPR, HIPAA, PCI DSS и др.) Владеет принципами и методами обеспечения безопасности информационных систем Владеет современными методами и технологиями в области безопасности ИС Знает источники угроз ИБ и меры по их предотвращению Ориентируется в принципах криптографии и шифрования данных (углублённо) Знает стандарты и протоколы безопасности (HTTPS, OAuth, OpenID Connect) Владеет основными принципами безопасности информации и методов её защиты Знает инструменты и технологии обеспечения безопасности (брандмауэры, IDS, антивирусы) Умеет определять этапы решения задачи, составлять план действий, определять ресурсы Умеет структурировать информацию, выделять значимое, оценивать практическую значимость Умеет шифровать данные и обеспечивать конфиденциальность Может разрабатывать и реализовывать меры безопасности Может реализовывать хэширование паролей, сессионные токены и 2FA 4 (Хорошо) Знает алгоритмы	
--	---	--

- основные принципы безопасности информации и методов ее защиты; - стандартные криптографические алгоритмы для шифрования данных; - принципы обеспечения безопасности передачи данных по сети; - основы безопасности приложений и инфраструктуры; - методы анализа на уязвимости и мониторинга безопасности; - знание основных принципов и методов обеспечения безопасности ИТ-инфраструктуры и веб-приложений; - понимание различных уязвимостей и угроз безопасности, а также способов их предотвращения и обнаружения; - знание инструментов и технологий для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы. Умеет: -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; - определять необходимые ресурсы; - владеть актуальными методами работы в профессиональной и смежных сферах; - реализовывать составленный план; - оценивать результат и	выполнения работ в профессиональной и смежных областях Знает методы работы в профессиональной и смежных сферах (хорошо, но без акцента на критический выбор) Знает структуру плана для решения задач Знает приёмы структурирования информации Знает принципы безопасности хранения данных Знает принципы криптографии и методов шифрования данных (базовый уровень) Имеет представление об основных угрозах безопасности мобильных приложений Знает стандартные криптографические алгоритмы для шифрования данных Имеет представление о принципах обеспечения безопасности передачи данных по сети Знает основы безопасности приложений и инфраструктуры Знает методы анализа на уязвимости и мониторинга безопасности Знает основные принципы и методы обеспечения безопасности ИТ-инфраструктуры и веб-приложений Понимает различные уязвимости и угрозы безопасности, способы их предотвращения и обнаружения Может распознавать задачу/проблему в профессиональном и/или социальном контексте	
---	---	--

последствия своих действий (самостоятельно или с помощью наставника); - 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; - использовать современное программное обеспечение; - использовать различные цифровые средства для решения профессиональных задач; - понимать тексты на базовые профессиональные темы; - шифрование данных и обеспечивает их конфиденциальность; - анализировать требования безопасности информационных систем; - разрабатывать и реализовывать меры безопасности; - реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию.	Анализирует задачу и выделяет её составные части Может выявлять и эффективно искать информацию, необходимую для решения Может реализовывать составленный план Оценивает результат и последствия своих действий (самостоятельно или с помощью наставника) Умеет определять задачи для поиска информации, источники, планировать процесс поиска Оформляет результаты поиска и применяет средства ИТ для решения задач Может использовать современное ПО и различные цифровые средства Понимает тексты на базовые профессиональные темы Умеет анализировать требования безопасности информационных систем 3 (Удовлетворительно) Владеет лексическим минимумом, относящимся к описанию предметов, средств и процессов профессиональной деятельности (минимально — без нюансов) Знает отраслевую нормативную техническую документацию и источники информации (перечислить может, но применять системно — затрудняется) Знает современный отечественный и зарубежный опыт в профессиональной деятельности (обзорно, без критического анализа) Знает принципы	
--	---	--

	безопасности информационных систем (общие, декларативно) Знает законодательные и нормативные акты в области безопасности ИС (знает названия, но не всегда толкует) Знает законодательные и регуляторные требования к защите данных (GDPR, HIPAA — на уровне «слышал»)	
--	--	--