МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Казанский (Приволжский) федеральный университет»
Колледж Елабужского института (филиала) КФУ

УТВЕРЖДАЮ
Заместитель директора по
образовательной деятельности
_____ С.Ю. Бахвалов
«__» _____ 2026 г.
МП

Программа дисциплины (модуля)
ОП.05 Основы информационной безопасности

Специальность: 09.02.11 Разработка и управление программным обеспечением

Квалификация выпускника: Программист

Форма обучения: очная

На базе: основного общего образования

Язык обучения: русский

Год начала обучения по образовательной программе: 2026

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ
«ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

1.1. Цель и место дисциплины в структуре образовательной программы

Цель дисциплины «Основы информационной безопасности»: формирование у студентов знаний и представлений о смысле, целях и задачах информационной защиты, характерных свойствах защищаемой информации, основных информационных угрозах, существующих направлениях защиты и возможностях построения моделей, стратегий, методов и правил информационной защиты.

Дисциплина «Основы информационной безопасности» включена в обязательную часть общепрофессионального цикла образовательной программы.

1.2. Планируемые результаты освоения дисциплины

Результаты освоения дисциплины соотносятся с планируемыми результатами освоения образовательной программы, представленными в матрице компетенций выпускника (п. 4.3 ПОП).

В результате освоения дисциплины обучающийся должен[1]:

Код компетенции	Умения	Знания	Владеть навыками
ОК - 01	применять положения компетенции ОК - 01 при освоении дисциплины «Основы информационной безопасности» и выполнении учебных и профессионально ориентированных заданий; Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	содержание компетенции ОК - 01; способы применения знаний дисциплины «Основы информационной безопасности» в профессиональной деятельности по специальности 09.02.11.	применения изученного материала при решении профессионально ориентированных учебных задач
ПК 4.7	выявлять угрозы безопасности ИТ-инфраструктуры; применять базовые организационные и технические меры защиты; использовать средства контроля доступа, резервного копирования, антивирусной защиты и мониторинга;	источники угроз ИТ-инфраструктуры; принципы защиты информации; методы аутентификации, авторизации, шифрования, резервного копирования и мониторинга безопасности;	применения мер защиты ИТ-инфраструктуры и контроля соблюдения требований информационной безопасности

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Трудоемкость освоения дисциплины

Наименование составных частей дисциплины	Объем в часах	Данные по учебному плану
Объем образовательной программы учебной дисциплины	72	всего
Учебные занятия	48	контактная работа
в том числе лекции	24	по учебному плану
практические занятия	24	по учебному плану
Самостоятельная работа	24	по учебному плану
Промежуточная аттестация	0	зачет с оценкой в 3 семестре
Всего	**72**	**по учебному плану**

2.2. Содержание дисциплины

Наименование разделов и тем	Содержание учебного материала, практических и лабораторных занятий с указанием часов по учебному плану
Итого по разделу по учебному плану: 72 ч. Компетенции: ОК - 01, ПК 4.7. Раздел 1. Основы информационной безопасности (72 часов)	
Тема 1.1. Введение в информационную безопасность	Объем темы по учебному плану: 8 ч. Компетенции: ОК - 01, ПК 4.7. Содержание
	Основные понятия и определения. История и развитие информационной безопасности. Актуальные угрозы и риски в информационной безопасности
	В том числе самостоятельная работа обучающихся *Необходимость и тематика определяются образовательной организацией*
Тема 1.2. Управление безопасностью информации	Объем темы по учебному плану: 8 ч. Компетенции: ОК - 01, ПК 4.7. Содержание
	Нормативно-правовое регулирование в области ИБ. Политики и процедуры безопасности. Оценка рисков и управление ими. Соответствие стандартам и нормативам (ISO 27001, GDPR и др.)
	В том числе самостоятельная работа обучающихся *Необходимость и тематика определяются образовательной организацией*
Тема 1.3. Криптография	Объем темы по учебному плану: 7 ч. Компетенции: ОК - 01, ПК 4.7. Содержание
	Основы криптографии: симметричные и асимметричные алгоритмы. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография.
	В том числе практических и лабораторных занятий
	Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой подписи сообщения.
	В том числе самостоятельная работа обучающихся *Необходимость и тематика определяются образовательной организацией*
Тема 1.4. Защита сетевой инфраструктуры	Объем темы по учебному плану: 7 ч. Компетенции: ОК - 01, ПК 4.7. Содержание
	Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.) Использование VPN и межсетевых экранов
	В том числе практических и лабораторных занятий
	Организация защиты от атак
	Организация работы VPN и межсетевого экрана
	В том числе самостоятельная работа обучающихся *Необходимость и тематика определяются образовательной организацией*
Тема 1.5. Безопасность приложений	Объем темы по учебному плану: 7 ч. Компетенции: ОК - 01, ПК 4.7. Содержание
	Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей.
	В том числе практических и лабораторных занятий
	Тестирование на проникновение и анализ уязвимостей.
	В том числе самостоятельная работа обучающихся *Необходимость и тематика определяются образовательной организацией*
Тема 1.6. Защита данных	Объем темы по учебному плану: 7 ч. Компетенции: ОК - 01, ПК 4.7. Содержание
	Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных. Управление доступом к данным
	В том числе практических и лабораторных занятий

	Выполнение резервного копирования и восстановления данных. Управление доступом к данным
	В том числе самостоятельная работа обучающихся *Необходимость и тематика определяются образовательной организацией*
Тема 1.7. Безопасность облачных технологий	Объем темы по учебному плану: 7 ч. Компетенции: ОК - 01, ПК 4.7. Содержание
	Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности
	В том числе практических и лабораторных занятий
	Изучение модели облачных услуг и их безопасности
	В том числе самостоятельная работа обучающихся *Необходимость и тематика определяются образовательной организацией*
Тема 1.8. Инциденты безопасности	Объем темы по учебному плану: 7 ч. Компетенции: ОК - 01, ПК 4.7. Содержание
	Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента. Кибербезопасность. Промышленный шпионаж. OSINT. Форензика
	В том числе практических и лабораторных занятий
	Работа с инцидентами.
	В том числе самостоятельная работа обучающихся *Необходимость и тематика определяются образовательной организацией*
Тема 1.9. Социальная инженерия и человеческий фактор	Объем темы по учебному плану: 7 ч. Компетенции: ОК - 01, ПК 4.7. Содержание
	Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности
	В том числе практических и лабораторных занятий
	Разработка политики информационной безопасности
	В том числе самостоятельная работа обучающихся *Необходимость и тематика определяются образовательной организацией*
Тема 1.10. Будущее информационной безопасности	Объем темы по учебному плану: 7 ч. Компетенции: ОК - 01, ПК 4.7. Содержание
	Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности
	В том числе самостоятельная работа обучающихся *Необходимость и тематика определяются образовательной организацией*
Промежуточная аттестация	
Всего 32 часа	
Итого по дисциплине	**Объем образовательной программы: 72 ч.; учебные занятия: 48 ч.; лекции: 24 ч.; лабораторные занятия: 0 ч.; практические занятия: 24 ч.; курсовой проект (работа): 0 ч.; консультации: 0 ч.; самостоятельная работа: 24 ч.; промежуточная аттестация: 0 ч.; форма контроля: зачет с оценкой в 3 семестре. Компетенции: ОК - 01, ПК 4.7.**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение

Лаборатория «Компьютерных сетей и основ информационной безопасности», оснащенная в соответствии с приложением 3 ПОП.

3.2. Учебно-методическое обеспечение

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 организации 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 и/или электронные издания

1. Баланов, А. Н. Защита информационных систем. Кибербезопасность : учебное пособие для спо / А. Н. Баланов. — Санкт-Петербург : Лань, 2024. — 84 с. — ISBN 978-5-507-48808-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/394547 (дата обращения: 16.11.2024).

2. Баланов, А. Н. Комплексная информационная безопасность : учебное пособие для спо / А. Н. Баланов. — Санкт-Петербург : Лань, 2024. — 284 с. — ISBN 978-5-507-49251-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/414950 (дата обращения: 16.11.2024).

3. Нестеров, С. А. Основы информационной безопасности : учебник для спо / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-9489-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/195510 (дата обращения: 16.11.2024)

4. Прохорова, О. В. Информационная безопасность и защита информации : учебник для спо / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург : Лань, 2024. — 124 с. — ISBN 978-5-507-47517-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/385082 (дата обращения: 16.11.2024)

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Результаты обучения	Показатели освоенности компетенций	Методы оценки
Освоение результатов дисциплины «Основы информационной безопасности» по компетенциям: ОК - 01, ПК 4.7.	Обучающийся выполняет учебные и практико-ориентированные задания, демонстрирует понимание содержания дисциплины, применяет знания при решении задач, предусмотренных учебным планом.	Текущий контроль, практические и лабораторные работы, тестирование, защита индивидуальных заданий; промежуточная аттестация: зачет с оценкой в 3 семестре.
Итоговые показатели	Сформированность знаний, умений и навыков оценивается по полноте, правильности, самостоятельности выполнения заданий и применимости результата к профессиональной деятельности.	Экспертное наблюдение, проверка письменных и практических работ, устный опрос, тестирование, экзамен/зачет согласно учебному плану.

5. Образовательные технологии

При реализации дисциплины ОП.05 «Основы информационной безопасности» используются традиционные, практико-ориентированные, проблемные, активные и интерактивные образовательные технологии. Основу занятий составляют лекции, практические занятия, анализ угроз информационной безопасности, решение ситуационных задач, выполнение индивидуальных и групповых заданий, работа с нормативными и учебными материалами.

Занятия, проводимые в активной и интерактивной формах

Номер темы	Наименование темы	Форма проведения занятия	Объем в часах
Тема 1	Основные понятия информационной безопасности	Проблемная лекция с анализом примеров угроз	2
Тема 2	Угрозы информационной безопасности	Кейс-задание по выявлению угроз и уязвимостей	2

Тема 3	Защита информации	Практическая работа по выбору средств защиты	2
Тема 4	Пароли и учетные записи	Практикум по правилам безопасной аутентификации	2
Тема 5	Вредоносное программное обеспечение	Анализ ситуаций заражения и способов профилактики	2
Тема 6	Политика информационной безопасности	Групповое задание по разработке правил безопасности	2
Всего			12

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

6.1. Оценочные средства для текущего контроля успеваемости

Текущий контроль проводится в ходе изучения разделов и тем дисциплины. Формами текущего контроля являются:

– устный опрос;
– тестирование;
– практические задания;
– анализ ситуационных задач;
– разработка памяток;
– составление правил информационной безопасности;
– контрольная работа;

Примерные вопросы для устного опроса:

1. Что понимается под информационной безопасностью?
2. Что такое конфиденциальность информации?
3. Что такое целостность информации?
4. Что такое доступность информации?
5. Какие угрозы информационной безопасности существуют?
6. Что такое уязвимость информационной системы?
7. Что такое вредоносное программное обеспечение?
8. Какие признаки имеет фишинговое сообщение?
9. Что такое социальная инженерия?
10. Какие требования предъявляются к надежному паролю?
11. Для чего используется двухфакторная аутентификация?
12. Что такое персональные данные?
13. Какие меры помогают защитить персональные данные?
14. Что такое резервное копирование?

Примерные тестовые задания:

1. Конфиденциальность информации означает:

Правильный ответ: защиту информации от несанкционированного доступа.

2. Фишинг — это:

Правильный ответ: попытка получить конфиденциальные данные обманным путем.

3. Надежный пароль должен:

Правильный ответ: содержать разные типы символов и не быть очевидным.

Практическая работа № 1. Анализ угроз информационной безопасности

Задание:

1. Определить защищаемый информационный актив.
2. Выявить возможные угрозы и уязвимости.
3. Описать возможные последствия.
4. Предложить меры защиты и оформить результат в таблице.

Критерии оценивания: оценка «5» выставляется при полном и правильном выполнении задания, наличии обоснованного вывода и аккуратном оформлении; «4» — при наличии отдельных неточностей; «3» — при частичном выполнении задания при подтверждении основных умений; «2» — при невыполнении задания или существенных ошибках.

Практическая работа № 2. Оценка надежности паролей

Задание:

1. Проанализировать варианты паролей.
2. Определить слабые и надежные пароли.
3. Составить правила создания надежного пароля.
4. Предложить способ безопасного хранения паролей.

Критерии оценивания: оценка «5» выставляется при полном и правильном выполнении задания, наличии обоснованного вывода и аккуратном оформлении; «4» — при наличии отдельных неточностей; «3» — при частичном выполнении задания при подтверждении основных умений; «2» — при невыполнении задания или существенных ошибках.

Практическая работа № 3. Выявление признаков фишинга

Задание:

1. Проанализировать текст сообщения.
2. Найти признаки мошенничества.
3. Определить, какие данные пытаются получить злоумышленники.
4. Составить безопасный алгоритм действий пользователя.

Критерии оценивания: оценка «5» выставляется при полном и правильном выполнении задания, наличии обоснованного вывода и аккуратном оформлении; «4» — при наличии отдельных неточностей; «3» — при частичном выполнении задания при подтверждении основных умений; «2» — при невыполнении задания или существенных ошибках.

Практическая работа № 4. Разработка памятки по защите персональных данных

Задание:

1. Определить виды персональных данных.
2. Указать риски их разглашения.
3. Сформулировать правила безопасной работы с персональными данными.
4. Оформить памятку для пользователя.

Критерии оценивания: оценка «5» выставляется при полном и правильном выполнении задания, наличии обоснованного вывода и аккуратном оформлении; «4» — при наличии отдельных неточностей; «3» — при частичном выполнении задания при подтверждении основных умений; «2» — при невыполнении задания или существенных ошибках.

Общие критерии оценивания текущего контроля:

Оценка «5» выставляется, если задание выполнено полностью, результат соответствует условию, вывод обоснован, оформление соответствует требованиям преподавателя.

Оценка «4» выставляется, если задание выполнено в основном верно, но имеются отдельные неточности, не искажающие общий результат.

Оценка «3» выставляется, если задание выполнено частично, имеются ошибки, но освоение основных элементов подтверждено.

Оценка «2» выставляется, если задание не выполнено или результат не подтверждает освоение материала.

6.2. Оценочные средства для промежуточной аттестации

Промежуточная аттестация по дисциплине ОП.05 «Основы информационной безопасности» проводится в форме: зачет с оценкой в 3 семестре.

Цель промежуточной аттестации — определить уровень освоения содержания дисциплины, сформированность практических умений, способность применять изученный материал при решении учебных и профессионально ориентированных задач, аргументировать решение и оформлять результат в соответствии с требованиями преподавателя.

Форма проведения промежуточной аттестации:

1. Ответ на теоретический вопрос.
2. Выполнение практического, расчетного или ситуационного задания.
3. Объяснение хода выполнения задания.
4. Формулировка вывода по результатам работы.

Примерные вопросы для промежуточной аттестации:

1. Понятие информационной безопасности.
2. Конфиденциальность, целостность и доступность информации.
3. Информационные активы.
4. Угрозы информационной безопасности.
5. Уязвимости информационных систем.
6. Вредоносное программное обеспечение.
7. Социальная инженерия.
8. Фишинг.
9. Парольная защита.
10. Двухфакторная аутентификация.
11. Защита персональных данных.
12. Безопасная работа с электронной почтой.
13. Резервное копирование.
14. Антивирусная защита.
15. Политика информационной безопасности.

Примерные практические задания для промежуточной аттестации:

1. Выявить угрозы в предложенной ситуации.
2. Оценить надежность пароля.
3. Найти признаки фишингового сообщения.
4. Составить правила защиты учетной записи.
5. Разработать меры защиты персональных данных.

Критерии оценивания промежуточной аттестации:

Оценка «отлично» выставляется, если обучающийся полно раскрывает теоретический вопрос, правильно выполняет практическое задание, обосновывает ход решения, использует профессиональную терминологию и делает корректный вывод.

Оценка «хорошо» выставляется, если ответ и практическое задание выполнены в целом верно, но имеются отдельные неточности в терминологии, расчетах, настройках, оформлении или аргументации.

Оценка «удовлетворительно» выставляется, если обучающийся раскрывает вопрос частично, показывает общее понимание темы, но допускает ошибки при выполнении задания.

Оценка «неудовлетворительно» выставляется, если обучающийся не владеет основными понятиями дисциплины и не может выполнить практическое задание.

7. Методические указания для обучающихся при освоении дисциплины

При освоении дисциплины ОП.05 «Основы информационной безопасности» обучающимся необходимо регулярно посещать учебные занятия, вести конспект, своевременно выполнять практические и самостоятельные задания, работать с основной и дополнительной литературой, электронными образовательными ресурсами и материалами преподавателя.

На лекционных занятиях следует фиксировать основные понятия, определения, классификации, формулы, алгоритмы действий, примеры выполнения заданий и типовые ошибки, на которые обращает внимание преподаватель.

Перед практическими занятиями необходимо повторять теоретический материал, изучать условия заданий, подбирать необходимые источники информации, готовить таблицы, схемы, файлы или иные материалы, необходимые для выполнения работы.

При выполнении практических заданий следует внимательно анализировать условие, записывать исходные данные, выполнять действия последовательно, проверять результат, оформлять работу в соответствии с требованиями преподавателя и формулировать вывод.

При выполнении кейсов необходимо определить информационный актив, угрозу, уязвимость, последствия и меры защиты. Не допускается использование реальных паролей и персональных данных при выполнении учебных заданий.

Самостоятельная работа обучающихся включает изучение учебной литературы, подготовку к устным опросам и тестированию, выполнение заданий, анализ ошибок, подготовку отчетов, повторение основных понятий и подготовку к промежуточной аттестации.

При подготовке к промежуточной аттестации необходимо повторить основные темы дисциплины, разобрать выполненные практические задания, устранить пробелы в знаниях и выполнить тренировочные задания по каждому разделу.

8. Материально-техническое и программное обеспечение дисциплины

Для реализации дисциплины ОП.05 «Основы информационной безопасности» используется учебный кабинет или лаборатория, обеспечивающие проведение лекционных и практических занятий, индивидуальной и групповой работы обучающихся, текущего контроля и промежуточной аттестации.

Материально-техническое обеспечение дисциплины включает:

– рабочее место преподавателя;

– рабочие места обучающихся;

– комплект учебной мебели;

– доску аудиторную или интерактивную панель;

– мультимедийное оборудование для демонстрации презентаций, схем, таблиц и учебных материалов;

– персональные компьютеры или ноутбуки при необходимости выполнения практических заданий;

– локальную сеть и доступ к информационно-телекоммуникационной сети Интернет;

– комплект раздаточных, справочных и методических материалов преподавателя;

Практические задания выполняются в учебной среде; при моделировании угроз не допускается использование вредоносного программного обеспечения и действий, нарушающих работу информационных систем.

Программное обеспечение дисциплины включает:

– операционная система;

– пакет офисных программ;

– браузер;

– средства просмотра PDF-документов;

– антивирусное программное обеспечение;

– средства архивации и резервного копирования при наличии;

– электронные образовательные ресурсы;

Материально-техническое и программное обеспечение должно обеспечивать возможность проведения занятий, выполнения практических заданий, оформления

отчетов, подготовки самостоятельной работы и проведения контроля результатов освоения дисциплины.

9. Учебно-методическое и информационное обеспечение дисциплины

9.1. Основная литература

1. Основы информационной безопасности: учебное пособие для среднего профессионального образования. — Москва: Юрайт, 2026.
2. Основы информационной безопасности: практикум для СПО. — Москва: КноРус, 2026.

9.2. Дополнительная литература

1. Методические материалы преподавателя для практических и самостоятельных работ.
2. Федеральные государственные образовательные стандарты СПО и локальные нормативные документы образовательной организации.

9.3. Интернет-ресурсы

1. Электронно-библиотечная система Znanium. — URL: https://znanium.ru (дата обращения: 24.06.2026). — Текст : электронный.
2. Электронно-библиотечная система «Лань». — URL: https://e.lanbook.com (дата обращения: 24.06.2026). — Текст : электронный.
3. Электронно-библиотечная система «Юрайт». — URL: https://urait.ru (дата обращения: 24.06.2026). — Текст : электронный.

10. Методы обучения для обучающихся инвалидов и лиц с ограниченными возможностями здоровья

Для обучающихся инвалидов и лиц с ограниченными возможностями здоровья создаются специальные условия освоения дисциплины с учетом индивидуальных особенностей, рекомендаций психолого-медико-педагогической комиссии и индивидуальной программы реабилитации или абилитации при ее наличии. Образовательный процесс может включать адаптацию темпа изучения материала, увеличение времени на выполнение заданий, предоставление материалов в электронном виде, использование технических средств обучения и индивидуальное консультирование.

При проведении текущего контроля и промежуточной аттестации допускается применение специальных технических средств, изменение формы представления задания, увеличение времени выполнения работы, использование ассистивных технологий и иных условий, не снижающих требования к результатам освоения дисциплины.

Программа составлена в соответствии с требованиями ФГОС СПО по специальности 09.02.11 «Разработка и управление программным обеспечением».