

**Автономная некоммерческая организация профессионального образования
«ПЕРМСКИЙ ГУМАНИТАРНО-ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ»
(АНО ПО «ПГТК»)**

УТВЕРЖДЕНА
Педагогическим советом АНО ПО «ПГТК»
(протокол от 05.02.2026 № 01)
Председатель Педагогического совета, директор
И.Ф. Никитина



**РАБОЧАЯ ПРОГРАММА
УЧЕБНОЙ ДИСЦИПЛИНЫ**

ОП.05 «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

для специальности

09.02.11 Разработка и управление программным обеспечением
(код и наименование специальности)

Квалификация выпускника
Программист

Форма обучения
Очная

Пермь 2026

Рабочая программа учебной дисциплины ОП.05 «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» составлена в соответствии с требованиями Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.11 Разработка и управление программным обеспечением (утвержден приказом Министерства Просвещения Российской Федерации от 24 февраля 2025 г. N 138).

Программа предназначена для студентов и преподавателей АНО ПО «ПГТК».

Автор – составитель: Могильникова Н.С., старший преподаватель.

Рабочая программа учебной дисциплины рассмотрена и одобрена на заседании кафедры математических и естественно-научных дисциплин, протокол, № 01 от 04.02.2026.

ОГЛАВЛЕНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ.....	3
2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ	5
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ.....	9
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ	11

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1 Область применения программы

Рабочая программа учебной дисциплины ОП.05 «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности 09.02.11 Разработка и управление программным обеспечением. Рабочая программа составлена для очной формы обучения.

1.2 Место дисциплины в структуре программы подготовки специалистов среднего звена

Учебная дисциплина ОП.05 «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» включена в обязательную часть общепрофессионального цикла программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности 09.02.11 Разработка и управление программным обеспечением.

1.3 Цели и задачи дисциплины – требования к результатам освоения дисциплины:

Цель дисциплины «ОП.05 Основы информационной безопасности»: формирование представлений области информационной безопасности, определяющей потребности в развитии интереса к изучению учебных дисциплин и профессиональных модулей, способности к личному самоопределению и самореализации в учебной деятельности.

В результате освоения дисциплины обучающийся должен:

Код ОК, ПК	Уметь	Знать
ОК. 01 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам; ОК. 02 Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности; ОК. 09 Пользоваться профессиональной документацией на государственном и	<ul style="list-style-type: none">• классифицировать защищаемую информацию по видам тайны и степеням секретности;• классифицировать основные угрозы безопасности информации	<ul style="list-style-type: none">• сущность и понятие информационной безопасности, характеристику ее составляющих;• место информационной безопасности в системе национальной безопасности страны;• виды, источники и носители защищаемой информации;• источники угроз безопасности информации и меры по их предотвращению;• факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;• жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;

иностранном языках.		<ul style="list-style-type: none"> • современные средства и способы обеспечения информационной безопасности; • основные методики анализа угроз и рисков информационной безопасности.
---------------------	--	--

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем, часов
Объем образовательной программы	72
В том числе:	
теоретическое обучение	32
практические занятия (в форме практической подготовки)	26
самостоятельная работа	12
промежуточная аттестация в форме дифференцированного зачета	2

2.2. Тематический план и содержание учебной дисциплины ОП.05 «Основы информационной безопасности»

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся, курсовая работа (проект)	Объем в часах	Осваиваемые компетенции
Раздел 1. Теоретические основы информационной безопасности			
Тема 1.1. Основные понятия и задачи информационной безопасности	Содержание Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем. Понятие «угроза информации». Понятие «риска информационной безопасности». Примеры преступлений в сфере информации и информационных технологий. Сущность функционирования системы защиты информации. Защита человека от опасной информации и от неинформированности в области информационной безопасности.	6	ОК.01, ОК.02, ОК.09
Тема 1.2. Основы защиты информации	Содержание Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи. Цели и задачи защиты информации. Основные понятия в области защиты информации. Элементы процесса менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации. Понятие политики безопасности.	6	ОК.01, ОК.02, ОК.09
	В том числе практические занятия (в форме практической подготовки): Определение объектов защиты на типовом объекте информатизации. Классификация защищаемой информации по видам тайны и степеням конфиденциальности.	6	
Тема 1.3. Угрозы безопасности защищаемой информации.	Содержание Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации. Каналы и методы несанкционированного доступа к уязвимости информации. Методы оценки уязвимости информации	6	ОК.01, ОК.02, ОК.09
	В том числе практические занятия (в форме практической подготовки):	8	

	Определение угроз объекта информатизации и их классификация		
Раздел 2. Методология защиты информации			
Тема 2.1. Методологические подходы к защите информации	Содержание Анализ существующих методик определения требований к защите информации. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации. Виды мер и основные принципы защиты информации.	4	ОК.01, ОК.02, ОК.09
Тема 2.2. Нормативно правовое регулирование защиты информации	Содержание Организационная структура системы защиты информации Законодательные акты в области защиты информации. Российские и международные стандарты, определяющие требования к защите информации. Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации	4	ОК.01, ОК.02, ОК.09
	В том числе практические занятия (в форме практической подготовки): Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности	6	
Тема 2.3. Защита информации в автоматизированных (информационных) системах	Содержание Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах. Программные и программно-аппаратные средства защиты информации Инженерная защита и техническая охрана объектов информатизации Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Принципы построения организационно-распорядительной системы.	6	ОК.01, ОК.02, ОК.09
	В том числе практические занятия (в форме практической подготовки): Выбор мер защиты информации для автоматизированного рабочего места	6	
Самостоятельная работа изучение литературы; осмысление изучаемой литературы; – работа в информационно-справочных системах; – аналитическая обработка текста (конспектирование, реферирование); – составление плана и тезисов ответа в процессе подготовки к занятию; – решение задач; – подготовка сообщений по вопросам семинарских занятий.		12	ОК.01, ОК.02, ОК.09

Промежуточная аттестация	Дифференцированный зачет	2	ОК.01, ОК.02, ОК.09
-----------------------------	--------------------------	---	------------------------

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Для реализации программы учебной дисциплины должны быть предусмотрены следующие специальные помещения:

Лаборатория "Программирования и баз данных" оснащенный оборудованием и техническими средствами обучения.

№	Наименование	Тип	Основное/ специализированно е
1.	рабочие места по количеству обучающихся	Мебель	основное
2.	рабочее место преподавателя	Мебель	основное
3.	персональный компьютер с программным обеспечением	Мебель	основное
4.	мультимедийный проектор	Оборудование	специализированное
5.	мультимедийный экран	Оборудование	специализированное
6.	наглядные пособия	ТС	специализированное
7.	Типовой состав для монтажа и наладки компьютерной сети: кабели различного типа, обжимной инструмент, коннекторы RJ-45, тестеры для кабеля, кросс-ножи, кросс-панели	ТС	специализированное

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы, рекомендуемые для использования в образовательном процессе

Основные источники:

1. Суворова, Г. М. Основы информационной безопасности : учебное пособие для СПО / Г. М. Суворова. — 2-е изд. — Саратов : Профобразование, 2024. — 135 с. — ISBN 978-5-4488-2237-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/142816.html>

2. 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 // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/124242.html>

Дополнительные источники:

1. Мельников, А. В. Основы информационной безопасности : учебное пособие / А. В. Мельников, С. В. Зарубин. — Москва : Российский государственный университет правосудия, 2025. — 220 с. — ISBN 978-5-00209-

188-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/152309.html>

2. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — 266 с. — ISBN 978-5-4497-3316-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/142285.html>

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

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

<i>Результаты обучения (освоенные умения, усвоенные знания)</i>	<i>Формы и методы контроля и оценки результатов обучения</i>
<p>В результате освоения дисциплины обучающийся знает:</p> <ul style="list-style-type: none">• сущность и понятие информационной безопасности, характеристику ее составляющих;• место информационной безопасности в системе национальной безопасности страны;• виды, источники и носители защищаемой информации;• источники угроз безопасности информации и меры по их предотвращению;• факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;• жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;• современные средства и способы обеспечения информационной безопасности;• основные методики анализа угроз и рисков информационной безопасности.	<p>Текущий контроль: индивидуальный и фронтальный опрос в ходе аудиторных занятий; оценка выполнения практических и индивидуальных заданий. Наблюдение за выполнением практического задания Оценка выполнения практического задания Дифференцированный зачет.</p>
<p>В результате освоения дисциплины обучающийся умеет:</p> <ul style="list-style-type: none">• классифицировать защищаемую информацию по видам тайны и степеням секретности;• классифицировать основные угрозы безопасности информации	

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п.п.	Содержание изменения	Дата, номер протокола заседания кафедры, подпись зав.кафедрой
1	2	3
1		
2		
3		
4		