**Министерство образования и науки Республики Татарстан**
**Государственное автономное профессиональное образовательное учреждение**
**«Сабинский аграрный колледж»**

**РАССМОТРЕНО** на заседании
предметной (цикловой) комиссии
Протокол № 4 от 15 апреля 2026 года

**ОДОБРЕНО**
на заседании Педагогического совета
ГАПОУ «САК»
протоколом №29 от «16» апреля 2026 года

# РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

## ОП.05 «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

для специальности

**09.02.11 «Разработка и управление программным обеспечением»**

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат: 1E093667AA5CBF33044A6008CC579BE5
Владелец: Бикмухаметов Закиржан Миннемуллович
Действителен с 02.09.2025 до 26.11.2026

**2026**

Рабочая программа учебной дисциплины ОП.05 «Основы информационной безопасности» разработана с учетом требований Федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности 09.02.11 «Разработка и управление программным обеспечением», утвержденного приказом Министерства просвещения Российской Федерации от 24.02.2025 года № 138 (зарегистрировано в Минюсте России 31.03.2025 года № 81696), укрупненная группа специальностей 09.00.00 «Информатика и вычислительная техника».

**СОДЕРЖАНИЕ**

# 1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

## ОП.05 «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

### 1.1. Место дисциплины в структуре основной образовательной программы среднего профессионального образования

Рабочая программа учебной дисциплины является частью основной образовательной программы подготовки специалистов среднего звена ГБПОУ «ПХТТ» в соответствии с ФГОС СПО по специальности 09.02.11 «Разработка и управление программным обеспечением».

Учебная дисциплина ОП.05 «Основы информационной безопасности» является обязательной дисциплиной общепрофессионального цикла основной образовательной программы.

### 1.2. Цели, задачи и планируемые результаты освоения дисциплины

#### 1.2.1. Цель и задачи учебной дисциплины

*Цель дисциплины «Основы информационной безопасности»:* формирование у обучающихся понимания основ информационной безопасности, практических навыков организации работ по обеспечению информационной безопасности на предприятиях и организациях.

*Задачи дисциплины:*

- способствовать освоению терминологического и понятийного аппарата теории информационной безопасности;
- изучить российское и зарубежное законодательство, а также особенности стандартов и спецификаций в области информационной безопасности;
- способствовать формированию знаний о возможных информационных угрозах и возможных средств защиты от них;
- изучить методологию и основные методы защиты информации от базовых угроз;
- способствовать формированию навыков оценки защищенности объектов и эффективности систем обеспечения информационной безопасности.

#### 1.2.2. Планируемые результаты освоения учебной дисциплины - требования к результатам освоения дисциплины

В рамках программы учебной дисциплины обучающимися формируются элементы общих компетенций (знания, умения). Планируемые результаты освоения дисциплины, направленные на формирование общих компетенций и подготовку к будущей профессиональной деятельности.

| Код компетенции | Наименование компетенции | Планируемые результаты (достижения образовательных результатов) | |
|---|---|---|---|
| | | **Умения** | **Знания** |
| ОК 01 | Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам | - применять аналитические навыки для диагностики и устранения неисправностей в работе информационных систем и сетей;<br>- точно описывать угрозу и документировать решение проблемы;<br>-выбирать меры защиты информации для автоматизированного рабочего места | - методы планирования своей работы;<br>- методы и приемы, используемые для недопущения/устранения угроз информационной безопасности |
| ОК 02 | Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности | - осуществлять поиск информации в открытых источниках и работать с технической документацией; | - методы и средства сбора информации и ее хранения;<br>- средства управления, связанные с использованием, обработкой, хранением и передачей данных; |
| ОК 09 | Пользоваться профессиональной документацией на государственном и иностранном языках | – читать или разрабатывать документацию к существующей или проектируемой информационной структуре предприятия | - законодательство в области информационной безопасности;<br>- отраслевые стандарты и системы профессиональных сертификаций; |
| ПК 1.5. | Защищать информацию в базе данных с использованием технологии защиты информации | - классифицировать основные угрозы безопасности информации;<br>- классифицировать защищаемую информацию по видам тайны и степеням секретности;<br>- выявлять информационные угрозы и;<br>- - анализировать и разрабатывать процедуры интеграции, тестирования, эксплуатации, сопровождения механизмов информационной безопасности. | сущность и понятие информационной безопасности, характеристику ее составляющих;<br>место информационной безопасности в системе национальной безопасности страны;<br>- виды, источники и носители защищаемой информации; источники угроз безопасности информации и меры по их предотвращению;<br>- факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;<br>- жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, |

| Код компетенции | Наименование компетенции | Планируемые результаты (достижения образовательных результатов) | |
|---|---|---|---|
| | | Умения | Знания |
| | | | передачи; современные средства и способы обеспечения информационной безопасности;<br>- основные методики анализа угроз и рисков информационной безопасности. |

# 2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

## 2.1. Объем учебной дисциплины и виды учебной работы (очная форма обучения)

| Вид учебной работы | Объем в часах |
|---|---|
| **Объем образовательной программы учебной дисциплины всего,** | **34** |
| в т. ч.: | |
| **Работа обучающихся во взаимодействии с преподавателем** | **32** |
| - теоретическое обучение (Л) | 24 |
| - практические занятия (ПЗ) | 8 |
| - консультации | |
| - промежуточная аттестация | |
| - курсовая работа (проект) | - |
| **Самостоятельная работа обучающегося (СРО)** | **2** |
| **Промежуточная аттестация:** | |

## 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 | Объем часов | | | Коды ОК, ПК, формированию которых способствует элемент программы |
|---|---|---|---|---|---|
| | | л | пр | сам | |
| 1 | 2 | 3 | | | 4 |
| **Раздел 1** | **Теоретические основы информационной безопасности** | **14** | | | |
| **Тема 1.1 Основные понятия и задачи информационной безопасности** | **Содержание** | | | | ОК 01 ОК 02 ОК 09 ПК 1.5 |
| | Введение в дисциплину | **2** | | | |
| | Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем. | **2** | | | |
| | Понятия компонента, класса и семейства | **1** | | | |
| | Объективно-ориентированный подход к информационной безопасности | **1** | | | |
| **Тема 1.2 Нормативно-правовое регулирование защиты информации** | **Содержание** | | | | ОК 01 ОК 02 ОК 09 ПК 1.5 |
| | Российское законодательство в области информационной безопасности | **1** | | | |
| | Зарубежное законодательство в области информационной безопасности | **1** | | | |
| | Информационная безопасность распределенных систем. Администрирование средств безопасности | **1** | | | |
| | Стандарты и спецификации в области информационной безопасности | **1** | | | |
| **Тема 1.3 Классификация безопасности** | **Содержание** | | | | ОК 01 ОК 02 ОК 09 ПК 1.5 |
| | Основные понятия и механизмы информационной безопасности | **1** | | | |
| | Классы безопасности | **1** | | | |
| **Тема 1.4 Документооборот, как способ защиты информации** | **Содержание** | | | | ОК 01 ОК 02 ОК 09 ПК 1.5 |
| | Правила и порядок оформления документов | **1** | | | |
| | Документооборот и его организация | **1** | | | |
| **Раздел 2** | **Методология защиты информации** | **9** | | | |
| **Тема 2.1 Угрозы безопасности защиты информации и основы защиты информации** | **Содержание** | | | | ОК 01 ОК 02 ОК 09 ПК 1.5 |
| | Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации. Угрозы информационной безопасности | **1** | | | |

| Наименование разделов и тем | Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся | Объем часов | | | Коды ОК, ПК, формированию которых способствует элемент программы |
|---|---|---|---|---|---|
| | | л | пр | сам | |
| 1 | 2 | 3 | | | 4 |
| | Способы защиты информации<br>Аппаратные и программные средства обеспечения безопасности государства | 1 | | | |
| | Защита от информационных утечек | 1 | | | |
| | Технические каналы утечки информации, способы обнаружения и предупреждения утечки информации по техническим каналам связи | 1 | | | |
| | Защита информации, содержащей коммерческую, государственную и иные виды тайн | 1 | | | |
| | Комплексные средства защиты информации | 1 | | | |
| **Тема2.2 Методологические подходы к защите информации** | **Содержание** | | | | ОК 01<br>ОК 02<br>ОК 09<br>ПК 1.5 |
| | Анализ существующих методик определения требований к защите информации. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации. | 1 | | | |
| | Виды мер и основные принципы защиты информации.<br>Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Принципы построения организационно-распорядительной системы. | 1 | | | |
| | Инженерная защита и техническая охрана объектов информатизации | 1 | | | |
| **Раздел 3** | **Практические занятия** | | 8 | | ОК 01<br>ОК 02<br>ОК 09<br>ПК 1.5 |
| | Порядок и оформление документов, документооборот | | 1 | | |
| | Определение объектов защиты на типовом объекте информатизации. | | 2 | | |
| | Классификация защищаемой информации по видам тайны и степеням конфиденциальности. | | 1 | | |
| | Определение угроз объекта информатизации и их классификация | | 1 | | |
| | Антивирусные программ и их использование. | | 1 | | |
| | Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности | | 1 | | |
| | Выбор мер защиты информации для автоматизированного рабочего места | | 1 | | |
| | | | | | |
| | **Итого** | 24 | 8 | | |

| Наименование разделов и тем | Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся | Объем часов | | | Коды ОК, ПК, формированию которых способствует элемент программы |
|---|---|---|---|---|---|
| | | л | пр | сам | |
| 1 | 2 | 3 | | | 4 |
| | Консультации | | | | |
| | Промежуточная аттестация (экзамен) | | | | |
| | Всего | 34 | | | |

# 3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

## 3.1. Требования к минимальному материально-техническому обеспечению

Кабинет «Общепрофессиональных дисциплин и профессиональных модулей», оснащенный:

- рабочее место преподавателя;
- персональный компьютер;
- посадочные места по количеству учащихся;
- мультимедийный проектор, экран;
- доска ученическая;

Программное обеспечение:
- ОС Windows 10 Pro для образовательных учреждений;
- Google Chrome
- MS Office Professional Plus 2019
- Visual Studio Community 2022
- WinRAR 5.40

## 3.2. Информационное обеспечение реализации программы

В процессе освоения программы дисциплины ОП.05 «Основы информационной безопасности» обучающимся предоставлена возможность доступа к электронным учебным материалам по дисциплине, имеющимся в свободном доступе в сети Интернет (электронным книгам, практикумам, тестам).

**Основные источники:**

1. Бубнов А.А. Основы информационной безопасности: учебник для студентов учреждений среднего профессионального образования /А.А. Бубнов, В.Н. Пржегорлинский, О.А. Савинкин. – М.: Издательский центр «Академия», 2018г.

2. Овчинникова, Е. А. Информационная безопасность. Организационно-правовые основы. В 2 частях. Ч. 1: учебное пособие для СПО / Е. А. Овчинникова, Г. В. Попков. — Саратов: Профобразование, 2024. — 191 с. — ISBN 978-5-4488-1876-9 (ч. 1), 978-5-4488-1883-7. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование: [сайт]. — URL: https://profspo.ru/books/139029

3. Овчинникова, Е. А. Информационная безопасность. Организационно-правовые основы. В 2 частях. Ч. 2: учебное пособие для СПО / Е. А. Овчинникова, Г. В. Попков. — Саратов: Профобразование, 2024. — 167 с. — ISBN 978-5-4488-1877-6 (ч. 2), 978-5-4488-1883-7. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование: [сайт]. — URL: https://profspo.ru/books/139030

4. Филиппов, Б. И. Информационная безопасность. Основы надежности средств связи: учебник / Б. И. Филиппов, О. Г. Шерстнева. — Саратов: Ай Пи Эр Медиа, 2019. — 227 с. — ISBN 978-5-4486-0485-0. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование: [сайт]. — URL: https://profspo.ru/books/80290

5. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов: Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/87995

**Дополнительные источники:**

1. Васильева Т.Ю. Информационная безопасность: учебник / Васильева Т.Ю., Куприянов А.И., Мельников В.П. — Москва: КноРус, 2018. — 371 с. — ISBN 978-5-406-04906-8. — URL: https://book.ru/book/929884 (дата обращения: 22.04.2021). — Текст: электронный.

2. Газизов, А. Р. Управление информационной безопасностью: учебное пособие / А. Р. Газизов, С. Б. Петренкова, Д. В. Фатхи. — Ростов-на-Дону: Донской государственный технический университет, 2019. — 115 с. — ISBN 978-5-7890-1775-3. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование: [сайт]. — URL: https://profspo.ru/books/117771

3. Мельников В.П. Информационная безопасность: учебное пособие для студентов средних профессиональных учебных заведений. - М.: Издательский центр "Академия", 2010г.

4. Моргунов, А. В. Информационная безопасность: учебно-методическое пособие / А. В. Моргунов. — Новосибирск: Новосибирский государственный технический университет, 2019. — 83 с. — ISBN 978-5-7782-3918-0. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование: [сайт]. — URL: https://profspo.ru/books/98708

5. Смышляев, А. Г. Информационная безопасность. Лабораторный практикум: учебное пособие / А. Г. Смышляев. — Белгород: Белгородский

государственный технологический университет им. В.Г. Шухова, ЭБС АСВ, 2015. — 102 с. — ISBN 2227-8397. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование: [сайт]. — URL: https://profspo.ru/books/66655

6. Солонская, О. И. Средства защиты информации: учебное пособие для СПО / О. И. Солонская. — Саратов: Профобразование, 2022. — 88 с. — ISBN 978-5-4488-1504-1. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование: [сайт]. — URL: https://profspo.ru/books/125578

7. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие для студентов СПО. - М.: ИД "ФОРУМ": ИНФРА-М, 2016г.

**Электронные источники:**

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области техниче-ской защиты информации www.fstec.ru
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Справочно-правовая система «Консультант Плюс» www.consultant.ru
5. Справочно-правовая система «Гарант» www.garant.ru
6. Федеральный портал «Российское образование www.edu.ru
7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
8. Российский биометрический портал www.biometrics.ru
9. Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
10. Сайт Научной электронной библиотеки www.elibrary.ru

### 3.3. Общие требования к организации образовательного процесса

Учебные занятия по дисциплине проводятся по расписанию в соответствии с учебным планом по специальности 09.02.11 «Разработка и управление программным обеспечением», календарным графиком и программой дисциплины в учебных аудиториях, оснащенных необходимым учебным, методическим, информационным, программным обеспечением.

Основными формами организации учебного изучения дисциплины являются лекции и практические занятия, а также самостоятельная работа

обучающихся.

Лекции формируют у обучавшихся системное представление об изучаемых разделах дисциплины, обеспечивают усвоение ими основных дидактических единиц, а также способствуют развитию интеллектуальных способностей. Занятия теоретического цикла могут носит практико-ориентированный характер.

Практические занятия обеспечивают приобретение и закрепление необходимых навыков и умений, формирование компетенций, готовность к самостоятельной и индивидуальной работе.

Самостоятельная работа обучающихся проводится вне аудиторных часов; включает в себя работу с литературой, подготовку рефератов по выбранной теме, подготовку к практическим/лабораторным занятиям, способствует развитию познавательной активности, творческого мышления обучающихся, прививает навыки самостоятельного поиска информации, а также формирует способность и готовность к самомотивации, самосовершенствованию, самореализации и творческой адаптации.

В процессе освоения дисциплины используются активные и интерактивные формы проведения занятий с применением электронных образовательных ресурсов в сочетании с внеаудиторной работой для формирования и развития общих и профессиональных компетенций обучающихся.

Изучение теоретического материала проводится как в каждой группе, так и для нескольких групп (при наличии нескольких групп по специальности).

Оценка результатов освоения дисциплины осуществляется проведением текущего контроля и промежуточной аттестации.

Текущий контроль проводится преподавателем в процессе обучения. Текущий учет результатов освоения дисциплины производится в электронном журнале успеваемости.

По окончанию изучения дисциплины проводится промежуточная аттестация. Результаты промежуточной аттестации фиксируются в зачетно-экзаменационной ведомости по дисциплине.

При освоении дисциплины, в соответствии с учебным планом и расписанием, для всех желающих проводятся консультации.

С целью оказания помощи обучающимся при освоении теоретического и практического материала, выполнения самостоятельной работы разрабатываются методические материалы по дисциплине.

Образовательный процесс может быть организован с использованием электронного обучения и дистанционных технологий.

На сайте СДО Техникума размещается теоретический материал для самостоятельного изучения обучающимся, задания для выполнения практических работ, автоматизированные тесты и другие учебные материалы (https://test.phtt.ru/).

Рабочая программ дисциплины размещается на сайте Техникума https://phtt.ru/.

.

# 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

**Контроль и оценка результатов освоения учебной дисциплины и компетенций** осуществляется преподавателем в процессе проведения учебных занятий, текущего контроля и промежуточной аттестации.

Оценка качества оценка результатов освоения учебной дисциплины осуществляется в двух направлениях:

- оценка уровня освоения дисциплины (знания и умения);
- оценка компетенций обучающихся (достижение результатов освоения компетенций).

1) Контроль и оценка результатов освоения учебной дисциплины:

| Результаты обучения | Критерии оценки | Методы оценки |
|---|---|---|
| **Перечень знаний, осваиваемых в рамках дисциплины**<br>Критерии оценки: не менее 70% правильных ответов при оценке знаний | | |
| **Знать:**<br>- методы планирования своей работы;<br>- методы и приемы, используемые для недопущения/устранения угроз информационной безопасности<br>- методы и средства сбора информации и ее хранения;<br>- средства управления, связанные с использованием, обработкой, хранением и передачей данных;<br>- законодательство в области информационной безопасности;<br>- отраслевые стандарты и системы профессиональных сертификаций;<br>сущность и понятие информационной безопасности, характеристику ее составляющих;<br>место информационной безопасности в системе национальной безопасности страны;<br>- виды, источники и носители защищаемой информации; источники угроз безопасности информации и меры по их предотвращению;<br>- факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;<br>- жизненные циклы информации | демонстрирует знания методов планирования своей работы;<br>демонстрирует знание методов и приемов, используемых для недопущения/устранения угроз информационной безопасности<br>демонстрирует знание методов и средств сбора информации и ее хранения;<br>владеет средствами управления, связанными с использованием, обработкой, хранением и передачей данных;<br>демонстрирует знание законодательства в области информационной безопасности;<br>демонстрирует знание отраслевых стандартов и систем профессиональных сертификаций;<br>знает сущность и понятие информационной безопасности, характеристику ее составляющих;<br>осознает место информационной безопасности в системе национальной безопасности страны;<br>демонстрирует знание о видах, источниках и носителях защищаемой информации; источниках угроз безопасности информации и меры по их предотвращению;<br>осведомлен о факторах, | Оценка результатов устного опроса<br>Оценка результатов практической работы<br>Оценка результатов тестирования<br>Самооценка своего знания, осуществляемая обучающимися<br>Экспертное наблюдение за ходом выполнения учебных заданий |

| Результаты обучения | Критерии оценки | Методы оценки |
|---|---|---|
| ограниченного доступа в процессе ее создания, обработки, передачи; современные средства и способы обеспечения информационной безопасности;<br>- основные методики анализа угроз и рисков информационной безопасности. | воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;<br>знает жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи; современные средства и способы обеспечения информационной безопасности;<br>знает основные методики анализа угроз и рисков информационной безопасности. | |
| **Перечень умений, осваиваемых в рамках дисциплины**<br>Критерии оценки: демонстрация устойчивых умений | | |
| **Уметь:**<br>- применять аналитические навыки для диагностики и устранения неисправностей в работе информационных систем и сетей;<br>- точно описывать угрозу и документировать решение проблемы;<br>-выбирать меры защиты информации для автоматизированного рабочего места;<br>- осуществлять поиск информации в открытых источниках и работать с технической документацией;<br>– читать или разрабатывать документацию к существующей или проектируемой информационной структуре предприятия<br>- классифицировать основные угрозы безопасности информации;<br>- классифицировать защищаемую информацию по видам тайны и степеням секретности;<br>- выявлять информационные угрозы;<br>- анализировать и разрабатывать процедуры интеграции, тестирования, эксплуатации, сопровождения механизмов информационной безопасности. | демонстрирует аналитические навыки для диагностики и устранения неисправностей в работе информационных систем и сетей;<br>демонстрирует умение описывать угрозу и документировать решение проблемы;<br>выбирает эффективные меры защиты информации для автоматизированного рабочего места<br>эффективно осуществляет поиск информации в открытых источниках и работать с технической документацией;<br>демонстрирует навыки чтения и разработки документации к существующей или проектируемой информационной структуре предприятия<br>верно классифицирует основные угрозы безопасности информации;<br>демонстрирует умение классификации защищаемой информации по видам тайны и степеням секретности;<br>демонстрирует навыки выявления информационных угроз;<br>демонстрирует навыки анализа и разработки процедур интеграции, тестирования, эксплуатации, сопровождения механизмов информационной безопасности. | Оценка результатов устного опроса<br>Оценка результатов практической работы<br>Оценка результатов тестирования<br>Самооценка своего умения, осуществляемая обучающимися<br>Экспертное наблюдение за ходом выполнения учебных заданий |
| **Промежуточная аттестация: экзамен** | | |

2) Контроль и оценка результатов освоения общих/профессиональных компетенций:

| **Результаты (освоенные общие/профессиональные компетенции)** | **Основные показатели оценки результата** | **Формы и методы контроля и оценки** |
|---|---|---|
| ОК 01 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам | Выбор оптимальных и эффективных способов решения задач профессиональной деятельности применительно к различным контекстам | Наблюдение в процессе теоретических и практических занятий<br><br>Оценка результатов устного опроса<br><br>Оценка результатов практической работы<br><br>Промежуточная аттестация |
| ОК 02 Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности | Эффективный поиск, анализ и интерпретация необходимой информации; использование различных источников, включая электронные | |
| ОК 09 Пользоваться профессиональной документацией на государственном и иностранном языках | Демонстрация навыков чтения и составления профессиональной документации | |
| ПК 1.5. Защищать информацию в базе данных с использованием технологии защиты информации | Демонстрация эффективного использования технологий защиты информации для защиты систем от информационных угроз | |

Лист согласования к документу № 5/26 от 08.06.2026
Инициатор согласования: Фазылова А.А. Секретарь
Согласование инициировано: 08.06.2026 07:59

**Лист согласования** Тип согласования: **последовательное**

| N° | ФИО | Срок согласования | Результат согласования | Замечания |
|---|---|---|---|---|
| 1 | Бикмухаметов З.М. | | Подписано 08.06.2026 - 08:00 | - |