

МИНИСТЕРСТВО ОБРАЗОВАНИЯ КРАСНОЯРСКОГО КРАЯ

**КРАЕВОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«КРАСНОЯРСКИЙ КОЛЛЕДЖ ОТРАСЛЕВЫХ ТЕХНОЛОГИЙ И
ПРЕДПРИНИМАТЕЛЬСТВА»**

РАССМОТРЕНО
методической комиссией
протокол № 10 от 18.06.2026

УТВЕРЖДЕНО
Директор КГАПОУ «ККОТиП»
_____/Н. В. Журова/
Приказ № 01-55-1п от 29.06.2026

**ПРОГРАММА ПОДГОТОВКИ
СПЕЦИАЛИСТОВ СРЕДНЕГО ЗВЕНА**

09.02.12 Техническая эксплуатация и сопровождение информационных систем
на базе основного общего образования

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
ПО УЧЕБНОЙ ДИСЦИПЛИНЕ**

ОП.06 Основы информационной безопасности

Красноярск, 2026

СОСТАВ КОМПЛЕКТА

1. Паспорт фонда оценочных средств.....	3
1.1. Общие положения.....	3
2. Формы контроля и оценивания элементов учебной дисциплины	3
3. Результаты освоения дисциплины.....	3
3.1. Профессиональные компетенции, подлежащие проверке при выполнении задания.....	3
3.2. Общие компетенции, подлежащие проверке при выполнении задания	Ошибка! Закладка не определена.
3.3. Основные показатели оценки результатов.....	Ошибка! Закладка не определена.
4. Оценка освоения курса учебной дисциплины	5
4.1. Задания для проведения промежуточной аттестации по учебной дисциплине	6

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

1.1. Общие положения

Контрольно-измерительные материалы предназначены для проверки результатов освоения учебной дисциплины **ОП.06 Основы информационной безопасности** основной образовательной программы среднего профессионального образования по специальности 09.02.12 Техническая эксплуатация и сопровождение информационных систем

Контрольно-измерительные материалы предназначены для текущего и промежуточного контроля, оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины **ОП.06 Основы информационной безопасности**.

Формой промежуточной аттестации по учебной дисциплине является экзамен, который оценивается по пятибалльной шкале оценок.

2. ФОРМЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ ЭЛЕМЕНТОВ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контролируемые темы (разделы) учебной дисциплины	Форма контроля и оценивания	
	Текущий контроль	Промежуточная аттестация
Раздел 1. Теоретические основы информационной безопасности	Практические работы № 1–2, устный опрос	Дифференцированный зачет
Раздел 2. Организационно-технические меры защиты	Практические работы № 3–4, защита рефератов/сообщений	
Раздел 3. Безопасность в цифровой среде	Практические работы № 5–6, защита рефератов/сообщений	

3. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ

3.1. Профессиональные компетенции, подлежащие проверке при выполнении задания

В результате текущего контроля и оценки результатов освоения умений и знаний по учебной дисциплине **ОП. 06 Основы информационной безопасности** осуществляется комплексная проверка следующих компетенций:

осваиваются следующие умения и знания:

умения	Применять основные методы и средства защиты информации. Обеспечивать защиту информации в автоматизированных системах. Соблюдать требования нормативных правовых актов в области информационной безопасности. Использовать антивирусные средства и межсетевое экранирование.
знания	Сущность и основные понятия информационной безопасности. Классификацию угроз информации и методы их предотвращения. Правовые основы и организационные меры защиты информации. Принципы работы криптографических средств защиты. Основы защиты информации в компьютерных сетях.

Формируемые общие компетенции:

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 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях;

ОК 04. Эффективно взаимодействовать и работать в коллективе и команде;

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста;

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения;

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях;

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности;

ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.

Код	Наименование общих компетенций
ПК 1.1	Осуществлять сбор данных для выявления требований к типовой информационной системе в соответствии с техническим заданием

4.ОЦЕНКА ОСВОЕНИЯ КУРСА УЧЕБНОЙ ДИСЦИПЛИНЫ

Наименование контроля	Тема	Форма контроля
Промежуточная аттестация		Дифференцированный зачет в форме устного опроса

ПАКЕТ ДЛЯ ПРОВЕДЕНИЯ ДИФФЕРЕНЦИРОВАННОГО ЗАЧЕТА

Задание: Промежуточная аттестация в форме устного опроса

Условия выполнения задания

1. Место (время) выполнения задания: кабинет «Информатики и информационных технологий»
2. Максимальное время выполнения задания: 30 минут
3. Требования охраны труда: не входить в кабинет в верхней одежде, не включать ПК без разрешения преподавателя, при обнаружении любых неисправностей немедленно сообщить преподавателю
4. Оборудование: ручка, листок

Критерии оценки:

Оценка «2» выставляется студенту, обнаружившему существенные пробелы в знаниях основного учебно-программного материала, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий; давшему ответ, который не соответствует вопросу экзаменационного билета.

Оценка «3» выставляется студенту, обнаружившему знание основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, справляющемуся с выполнением заданий, предусмотренных программой; допустившему неточности в ответе, но обладающими необходимыми знаниями для их устранения под руководством преподавателя.

Оценка «4» соответствует следующей качественной характеристике: «изложено правильное понимание вопроса, дано достаточно подробное описание предмета ответа, приведены и раскрыты в тезисной форме основные понятия, относящиеся к предмету ответа, ошибочных положений нет». Выставляется студенту, обнаружившему полное знание учебно-программного материала, грамотно и по существу отвечающему на вопрос билета и не допускающему при этом существенных неточностей; показавшему систематический характер знаний по дисциплине и способному к их самостоятельному пополнению и обновлению в ходе дальнейшей учебы и профессиональной деятельности.

Оценка «5» соответствует следующей качественной характеристике: «изложено правильное понимание вопроса и дан исчерпывающий на него ответ, содержание раскрыто полно, профессионально, грамотно». Выставляется студенту, усвоившему взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии, проявившему творческие способности в понимании, изложении и использовании учебно-программного материала; обнаружившему всестороннее систематическое знание учебно-программного материала, четко и самостоятельно (без наводящих вопросов) отвечающему на вопрос билета.

4.1. Задания для проведения промежуточной аттестации по учебной дисциплине

Дифференцированный зачет по учебной дисциплине проводится в форме устного опроса

Список вопросов для проведения дифференцированного зачета

1. Определение, цели и задачи информационной безопасности. Основные понятия (информация, доступность, целостность, конфиденциальность).
2. Классификация угроз информации. Естественные и искусственные угрозы. Случайные и умышленные угрозы.
3. Каналы утечки информации и методы их предотвращения.
4. Модель нарушителя информационной безопасности. Виды нарушителей и их мотивация.
5. Законодательство РФ в области информационной безопасности. Обзор ФЗ «Об информации, информационных технологиях и о защите информации» (149-ФЗ).
6. Федеральный закон «О персональных данных» (152-ФЗ): основные понятия и требования к операторам.
7. Организационно-распорядительные документы в области информационной безопасности (Постановления Правительства, приказы ФСТЭК).
8. Ответственность за нарушения в сфере информационной безопасности (административная, уголовная, дисциплинарная).
9. Идентификация и аутентификация пользователей. Парольная защита: требования к сложности и сроку действия паролей.
10. Биометрические методы аутентификации: виды, преимущества и уязвимости.
11. Основы криптографии. Симметричные и асимметричные алгоритмы шифрования.
12. Электронная подпись: назначение, виды, применение.
13. Виды вредоносного программного обеспечения. Классификация вирусов, червей, троянов.
14. Антивирусные средства: методы обнаружения вредоносного ПО. Классификация антивирусных программ.
15. Основные типы сетевых атак: DoS/DDoS-атаки, sniffing, спуфинг, фишинг.
16. Межсетевое экранирование (брандмауэры): принцип работы, виды, правила настройки.
17. Виртуальные частные сети (VPN): назначение, принципы работы, использование для защиты данных.
18. Криптографическая защита данных на диске (шифрование дисков и файлов).
19. Угрозы в сети Интернет. Социальная инженерия и фишинг: методы и меры противодействия.
20. Правила безопасного поведения в сети Интернет (цифровая гигиена).
21. Стратегии резервного копирования данных. Виды резервного копирования (полное, дифференциальное, инкрементальное).
22. Планирование непрерывности бизнеса. Восстановление данных после сбоев и атак.
23. Особенности защиты информации в облачных сервисах. Модели ответственности провайдера и клиента.
24. Информационная безопасность мобильных устройств.
25. Защита информации в системах дистанционного банковского обслуживания.
26. Обеспечение безопасности при использовании электронной почты. Защита от спама и фишинга.
27. Инциденты информационной безопасности: классификация и порядок реагирования.
28. Методы и средства обнаружения вторжений (IDS/IPS).
29. Компьютерные преступления: виды и ответственность по Уголовному кодексу РФ (глава 28).
30. Авторское право в цифровой среде. Защита интеллектуальной собственности.
31. Этические аспекты сбора и обработки персональных данных.

- 32. Хакеры: мотивация, методы деятельности, различие между «белыми» и «черными» хакерами.
- 33. Политика информационной безопасности организации: структура, цели, внедрение.
- 34. Роль федеральных органов власти в обеспечении ИБ (ФСТЭК, Роскомнадзор, ФСБ).
- 35. Организация пропускного режима и физической защиты информации на предприятии.
- 36. Информационная безопасность в государственных информационных системах.