

**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



**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
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

Фонд оценочных средств учебной дисциплины ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ составлен 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.

Фонд оценочных средств учебной дисциплины рассмотрена и одобрена на заседании кафедры математических и естественно-научных дисциплин, протокол, № 01 от 04.02.2026

Содержание ФОС УД

1. Паспорт фонда оценочных средств
 - 1.1. Область применения фонда оценочных средств
 - 1.2. Организация текущего контроля успеваемости и промежуточной аттестации по итогам освоения учебной дисциплины
2. Контроль и оценка достижения запланированных результатов обучения
 - 2.1. Перечень вопросов и заданий для текущего контроля знаний
 - 2.2. Перечень вопросов и заданий для промежуточной аттестации

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

1.1 Область применения ФОС

Фонд оценочных средств предназначен для оценивания достижений запланированных результатов по дисциплине ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

Фонд оценочных средств (ФОС) представляет собой комплект материалов для проведения промежуточной аттестации и текущего контроля.

Результаты обучения - это усвоенные знания и освоенные умения по дисциплине в целях овладения предусмотренных стандартом общих и профессиональных компетенций, а также для оценки достижения обучающимися личностных результатов.

Фонд оценочных средств позволяет оценивать:

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 иностранном языках.	<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;• современные средства и способы обеспечения информационной безопасности;• основные методики анализа угроз и рисков информационной безопасности.

1.2. Организация текущего контроля успеваемости и промежуточной аттестации по итогам освоения программы учебной дисциплины

В период обучения по образовательной программе СПО осуществляется текущий контроль успеваемости студентов, промежуточная аттестация по учебным дисциплинам и МДК.

Текущий контроль осуществляется в пределах учебного времени, отведенного на учебную дисциплину, оценивается по пятибалльной шкале. Текущий контроль проводится с целью объективной оценки качества освоения программы дисциплины, а также стимулирования учебной деятельности студентов, подготовки к промежуточной аттестации и обеспечения максимальной эффективности учебного процесса. Для оценки качества

подготовки используются различные формы и методы контроля. Текущий контроль дисциплины осуществляется в форме устного опроса; защиты практических заданий, реферата, творческих работ; выполнения контрольных и тестовых заданий; решения ситуационных задач и других форм контроля, предусмотренных программой дисциплины.

Промежуточная аттестация проводится в форме, предусмотренной планом учебного процесса: экзамена, дифференцированного зачета, зачета.

В период сложной санитарно-эпидемиологической обстановки или других ситуациях невозможности очного обучения и проведения аттестации студентов колледж реализует образовательные программы или их части с применением электронного обучения, дистанционных образовательных технологий в предусмотренных законодательством формах обучения или при их сочетании, при проведении учебных занятий, практик, текущего контроля успеваемости, промежуточной аттестации обучающихся.

Форма промежуточной аттестации по дисциплине ОП.05 Основы информационной безопасности – дифференцированный зачет.

2. КОНТРОЛЬ И ОЦЕНКА ОСВОЕНИЯ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Перечень вопросов и заданий для текущего контроля

В результате текущей аттестации по учебной дисциплине ОП.05 Основы информационной безопасности осуществляется проверка сформированности умений и знаний, направленных на формирование соответствующих ФГОС СПО общих и профессиональных компетенций.

Инструкция по выполнению работы – тестирование

Варианты заданий:

1. В Законе РФ "Об участии в международном информационном обмене" информационная безопасность определяется как ...
2. Информационная безопасность - это комплекс мероприятий, обеспечивающий для охватываемой им информации следующие факторы:
 - а) конфиденциальность
 - б) целостность
 - в) доступность
 - г) учет
 - д) неотрекаемость
 - е) мобильность
3. ... - распознавание каждого участника процесса информационного взаимодействия перед тем, как к нему будут применены какие бы то ни было понятия информационной безопасности.
 - а) Политика
 - б) Идентификация
 - в) Аутентификация
 - г) Контроль доступа
 - д) Авторизация
4. ... - это набор формальных правил, которые регламентируют функционирование механизма информационной безопасности.
 - а) Политика
 - б) Идентификация
 - в) Аутентификация
 - г) Контроль доступа
 - д) Авторизация
5. По доступности информация классифицируется на:
 - а) открытую
 - б) информацию и государственную тайну
 - в) конфиденциальную информацию
 - г) информацию свободного доступа информацию с ограниченным доступом и общедоступную информацию виды информации, указанные в остальных пунктах
6. К информации ограниченного доступа не относится
 - а) государственная тайна
 - б) размер золотого запаса страны
 - в) персональные данные
 - г) коммерческая тайна
7. Действие Закона "О государственной тайне" распространяется
 - а) на всех граждан и должностных лиц РФ
 - б) только на должностных лиц
 - в) на граждан, которые взяли на себя обязательство выполнять требования
 - г) законодательства о государственной тайне
 - д) на всех граждан и должностных лиц, если им предоставили для работы закрытые

сведения

8. Классификация и виды информационных ресурсов определены

- а) Законом "Об информации, информатизации и защите информации"
- б) Гражданским кодексом
- в) Конституцией
- г) всеми документами, перечисленными в остальных пунктах

9. Государственные информационные ресурсы не могут принадлежать

- а) физическим лицам
- б) коммерческим предприятиям
- в) негосударственным учреждениям
- г) всем перечисленным субъектам

10. Вопросы информационного обмена регулируются (...) правом

- а) гражданским
- б) информационным
- в) конституционным
- г) уголовным

Критерии оценки

Оценка

«5» - 20-18

«4» - 17-14

«3» - 13-11

«2» - 10-0

Выполнение и защита практических заданий

Аттестация проводится в форме защиты практического задания по завершению освоения учебного материала раздела, к выполнению и защите практического задания допускаются все обучающиеся.

На выполнение практической работы отводится 60 минут, на защиту практической работы отводится 15-20 минут..

Варианты заданий:

Практическая работа №1. Определение угроз объекта информатизации и их классификация. Цель работы: освоение приемов и методов определения угроз объекта информатизации и их классификации.

Практическая работа №2. Анализ рисков для безопасности информационной системы и ее ресурсов предприятия, определение степени их допустимости.

Цель работы: освоение приемов и методов анализа и определения рисков для безопасности информационной системы и ее ресурсов предприятия, определение степени их допустимости.

Практическая работа №3. Составление модели нарушителей информационной безопасности, актуальных для данного предприятия.

Цель работы: освоение приемов и методов составления модели нарушителей информационной безопасности, актуальных для данного предприятия.

Критерии оценки

Оценка	Критерии
«Отлично»	Практических задания выполнены в полном объеме в соответствии с заданием.
«Хорошо»	Практических задания выполнены полностью в соответствии с заданием незначительными недочетами.
«Удовлетворительно»	Одно практическое задание выполнено в полном объеме в соответствии с заданием.
«Неудовлетворительно»	Не одно практическое задание не выполнено в полном объеме

2.2.Перечень вопросов и заданий для промежуточной аттестации

Форма: дифференцированный зачет

Примерная структура оценочного средства

Инструкция по выполнению работы

Обучающийся вытягивает карточку с вопросами (3 вопроса в карточке)

Готовиться в течение 30 минут и отвечает устно

Варианты вопросов:

1. Дайте характеристику составляющих "информационной безопасности" применительно к вычислительным сетям.
2. Перечислите основные механизмы безопасности.
3. Какие механизмы безопасности используются для обеспечения конфиденциальности трафика?
4. Какие механизмы безопасности используются для обеспечения "неотказуемости" системы?
5. Что понимается под администрированием средств безопасности?
6. Какие виды избыточности могут использоваться в вычислительных сетях?
7. Как обнаружить загрузочный вирус?
8. Характерные черты макровируса.
9. Является ли наличие скрытых листов в Excel признаком заражения макровирусом?
10. Перечислите наиболее распространенные пути заражения компьютеров вирусами.
11. Особенности заражения компьютеров локальных сетей.
12. Как ограничить заражение макровирусом при работе с офисными приложениями?
13. Как обнаружить резидентный вирус?
14. Как проверить систему на наличие макровируса?
15. Перечислите основные этапы алгоритма обнаружения вируса.
16. Какие особенности заражения вирусами при использовании электронной почты?
17. Перечислите основные правила защиты от компьютерных вирусов, получаемых не из вычислительных сетей.
18. Как ограничить заражение макровирусом при работе с офисными приложениями?
19. Как рассматривается сеть в концепции протокола IP?
20. Преобразуйте IP-адрес "11110011 10100101 00001110 11000001" в десятичную форму.
21. Из каких частей состоит IP-адрес?
22. Для чего предназначен DNS-сервер?
23. Перечислите классы удаленных угроз.
24. Как классифицируются удаленные угрозы "по характеру воздействия"?
25. Охарактеризуйте удаленные угрозы "по цели воздействия".
26. Дайте определение маршрутизатора.
27. Что такое подсеть и сегмент сети? Чем они отличаются?
28. Что такое IP-адрес?
29. Сколько классов сетей определяет IP протокол?
30. К какому классу относится следующий адрес: 199.226.33.168?
31. Какой из этих адресов не может существовать: 109.256.33.18 или 111.223.44.1?
32. Поясните понятие домена.
33. В чем заключается иерархический принцип системы доменных имен?
34. Как классифицируются удаленные угрозы "по расположению субъекта и объекта угрозы"?
35. Может ли пассивная угроза привести к нарушению целостности информации?
36. Что такое подсеть и сегмент сети? Чем они отличаются?
37. Перечислите основные причины успешной реализации удаленных угроз информационной безопасности в вычислительных сетях.
38. Почему виртуальное соединение не обеспечивает требуемого уровня защиты

вычислительных сетей?

39. Какая из причин приводит к успеху удаленной угрозы "анализ сетевого трафика"?
40. В чем заключаются преимущества сети с выделенными каналами?
41. Какие алгоритмы удаленного поиска Вам известны?
42. Какой из алгоритмов поиска более безопасный?
43. Что является следствием недостаточной аутентификации субъектов и объектов вычислительных сетей?
44. К чему приводит недостаточность информации об объектах вычислительной сети? Приведите пример.
45. Может ли быть нарушена целостность информации при отсутствии в распределенных вычислительных сетях возможности контроля за маршрутом сообщений? Почему?
46. Как повысить защищенность вычислительных сетей при установлении виртуального соединения?
47. Как можно защитить сеть от реализации атаки "отказ в обслуживании"?
48. Как можно контролировать маршрут сообщения в сети?
49. Классификация угроз информационной безопасности автоматизированных систем по базовым признакам.
50. Угроза нарушения конфиденциальности. Особенности и примеры реализации угрозы.
51. Угроза нарушения целостности данных. Особенности и примеры реализации угрозы.
52. Угроза отказа служб (угроза отказа в доступе). Особенности и примеры реализации угрозы.
53. Угроза раскрытия параметров системы. Особенности и примеры реализации угрозы.
54. Понятие политики безопасности информационных систем. Назначение политики безопасности.
55. Основные типы политики безопасности доступа к данным. Дискреционные и мандатные политики.
56. Требования к системам криптографической защиты: криптографические требования, требования надежности, требования по защите от НСД, требования к средствам разработки.
57. Законодательный уровень обеспечения информационной безопасности. Основные законодательные акты РФ в области защиты информации.
58. Функции и назначение стандартов информационной безопасности. Примеры стандартов, их роль при проектировании и разработке информационных систем.
59. Критерии оценки безопасности компьютерных систем («Оранжевая книга»). Структура требований безопасности. Классы защищенности.
60. Основные положения руководящих документов Гостехкомиссии России. Классификация автоматизированных систем по классам защищенности. Показатели защищенности средств вычислительной техники от несанкционированного доступа.
61. Единые критерии безопасности информационных технологий. Понятие профиля защиты. Структура профиля защиты.
62. Единые критерии безопасности информационных технологий. Проект защиты. Требования безопасности (функциональные требования и требования адекватности).
63. Административный уровень защиты информации. Задачи различных уровней управления в решении задачи обеспечения информационной безопасности.
64. Процедурный уровень обеспечения безопасности. Авторизация пользователей в информационной системе.
65. Идентификация и аутентификация при входе в информационную систему. Использование парольных схем. Недостатки парольных схем.

66. Идентификация и аутентификация пользователей. Применение программно-аппаратных средств аутентификации (смарт-карты, токены).
67. Биометрические средства идентификации и аутентификации пользователей.
68. Аутентификация субъектов в распределенных системах, проблемы и решения. Схема Kerberos.
69. Аудит в информационных системах. Функции и назначение аудита, его роль в обеспечении информационной безопасности.
70. Понятие электронной цифровой подписи. Процедуры формирования цифровой подписи.
71. Законодательный уровень применения цифровой подписи.
72. Методы несимметричного шифрования. Использование несимметричного шифрования для обеспечения целостности данных.
73. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
74. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.
75. Средства обеспечения информационной безопасности в ОС Windows'2000. Разграничение доступа к данным. Групповая политика.
76. Применение файловой системы NTFS для обеспечения информационной безопасности в Windows NT/2000/XP. Списки контроля доступа к данным (ACL) их роль в разграничении доступа к данным.
77. Применение средств Windows 2000/XP для предотвращения угроз раскрытия конфиденциальности данных. Шифрование данных. Функции и назначение EFS.
78. Разграничение доступа к данным в ОС семейства UNIX.
79. Пользователи и группы в ОС UNIX.
80. Пользователи и группы в ОС Windows'2000.
81. Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.
82. Причины нарушения безопасности информации при ее обработке криптографическими средствами.
83. Понятие атаки на систему информационной безопасности. Особенности локальных атак.
84. Распределенные информационные системы. Удаленные атаки на информационную систему.
85. Каналы передачи данных. Утечка информации. Атаки на каналы передачи данных.
86. Физические средства обеспечения информационной безопасности.
87. Электронная почта. Проблемы обеспечения безопасности почтовых сервисов и их решения.
88. Вирусы и методы борьбы с ними. Антивирусные программы и пакеты.
89. Программно-аппаратные защиты информационных ресурсов в Интернет. Межсетевые экраны, их функции и назначения.
90. Виртуальные частные сети, их функции и назначение.

3.1.4 Критерии оценки

Оценка	Критерии
«Отлично»	Практических задания выполнены в полном объеме в соответствии с заданием.
«Хорошо»	Практических задания выполнены полностью в соответствии с заданием незначительными недочетами.
«Удовлетворительно»	Одно практическое задание выполнено в полном объеме в соответствии с заданием.

«Неудовлетворительно»	Не одно практическое задание не выполнено в полном объеме
-----------------------	---