МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«Казанский государственный аграрный университет»
(ФГБОУ ВО Казанский ГАУ)

Институт экономики
Кафедра цифровых технологий и прикладной информатики

УТВЕРЖДАЮ
Проректор по учебной
работе и цифровизации, доцент
_____ А.В. Дмитриев
«23» октября 2025 г.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 742E1DCDED9986891498E050140C0918
Владелец: Дмитриев Андрей Владимирович
Действителен: с 21.04.2025 до 15.07.2026

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

«Информационная безопасность в профессиональной деятельности»
(Оценочные средства и методические материалы)

приложение к рабочей программе дисциплины

Направление подготовки
09.04.03 Прикладная информатика

Направленность (профиль) подготовки
Анализ данных и искусственный интеллект

Форма обучения
очная

Казань – 2025

Паспорт

оценочных материалов для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю) Информационная безопасность в профессиональной деятельности

Перечень оценочных материалов и индикаторов достижения компетенций, сформированность которых они контролируют

Наименование оценочного средства	Коды индикаторов достижения формируемых компетенций	Номер приложения
Выполнение заданий на практических работах	ИД-1 ПК-8 ИД-2 ПК-8	1
Зачет	ИД-1 ПК-8 ИД-2 ПК-8	2

Приложение 1

1. Текущий контроль

Тема	№ заданий (вопросов, билетов, тестов и пр.) для оценки результатов обучения по соотнесенному индикатору достижения компетенции
Тема 1, 2	Вопросы к зачёту с оценкой в устной форме 1-76 Вопросы к зачёту с оценкой в тестовой форме 1-10 Примеры заданий для контрольной работы 1-23
Тема 3, 4	Вопросы к зачёту с оценкой в устной форме 1-76 Вопросы к зачёту с оценкой в тестовой форме 10-25 Примеры заданий для контрольной работы 1-23

Приложение 2

Вопросы к зачёту в устной форме

1. Особенностями современных информационных технологий?
2. Когда появились первые преступления с использованием компьютерной техники в России?
3. Сколько уголовных дела по ст.272 УК РФ («Неправомерный доступ к компью терной информации») и ст. 165 УК РФ ("Причинение имущественного ущерба путем обмана и злоупотребления доверием") было возбуждено в 2003 году в России?
4. Какой ущерб нанесли компьютерные вирусы за последние 5 лет?
5. Что понимается под информационной безопасностью Российской Федерации?
6. Первая составляющая национальных интересов Российской Федерации в ин формационной сфере?
7. Вторая составляющая национальных интересов Российской Федерации в ин формационной сфере?
8. Третья составляющая национальных интересов Российской Федерации в инфор мационной сфере?
9. Четвертая составляющая национальных интересов Российской Федерации в ин формационной сфере?
10. Классификация компьютерных преступлений?
11. Экономические компьютерные преступления?
12. Компьютерными преступлениями против личных прав и частной сферы?
13. Компьютерные преступления против государственных и общественных интере сов?
14. Основные виды преступлений, связанных с вмешательством в работу компьюте ров?
15. Способы совершения компьютерных преступлений?
16. Методы перехвата компьютерной информации?
17. Пользователи и злоумышленники в Метет?
18. Кто такие хакеры?
19. Кто такиефракеры?

20. Защита инфо
21. Кто такиекракеры?
22. Кто такиефишеры?
23. Кто такиескамеры?
24. Кто такиеспамеры?
25. Причины уязвимости сети 1п1егпег?
26. Защищаемая информация это?
27. Защита информации это?
28. Защита информации от утечки это?
29. Защита информации от несанкционированного воздействия это?
30. Защита информации от непреднамеренного воздействия это?
31. Защита информации от разглашения это?
32. Защита информации от несанкционированного доступа это?
33. Защита информации от иностранной разведки это?
34. Защита информации от иностранной технической разведки это?
35. Защита информации от агентурной разведки это?
36. Цель защиты информации?
37. Эффективность защиты информации это?
38. Показатель эффективности защиты информации это?
39. Нормы эффективности защиты информации это?
40. Организация защиты информации это?
41. Система защиты информации это?
42. Мероприятие по защите информации это?
43. Мероприятие по контролю эффективности защиты информации это?
44. Техника защиты информации это?
45. Объект защиты это?
46. Способ защиты информации это?
47. Категорирование защищаемой информации это?
48. Метод контроля эффективности защиты информации это?
49. Контроль состояния защиты информации это?
50. Средство защиты информации это?
51. Средство контроля эффективности защиты информации это?
52. Контроль организации защиты информации это?
53. Контроль эффективности защиты информации это?
54. Организационный контроль эффективности защиты информации это?
55. Технический контроль эффективности защиты информации это?
56. Информация это?
57. Доступ к информации это?
58. Субъект доступа к информации это?
59. Носитель информации это?
60. Собственник информации это?
61. Владелец информации это?
62. Пользователь (потребитель) информации это?
63. Право доступа к информации это?
64. Правило доступа к информации это?
65. Орган защиты информации это?
66. Информационные процессы это?
67. Информационная система это?
68. Информационными ресурсами это?
69. Что понимают под утечкой информации?
70. Несанкционированный доступ это?
71. Несанкционированное воздействие это?

72. Что понимается под непреднамеренным воздействием на защищенную инфор мацию?
73. Что понимается под эффективностью защиты информации?
74. Конфиденциальность информации это?
75. Шифрование информации это?
76. Уязвимость информации это?

Вопросы к зачёту в устной форме

Вопрос 1. Какие основные цели преследует злоумышленник при несанкционированном доступе к информации?
1) получить, изменить, а затем передать ее конкурентам;
2) размножить или уничтожить ее;
3) получить, изменить или уничтожить;
4) изменить и уничтожить ее;
5) изменить, повредить или ее уничтожить.

Вопрос 2. Какая информация является охраняемой внутригосударственным законодательством или международными соглашениями как объект интеллектуальной собственности?
1) любая информация;
2) только открытая информация;
3) запатентованная информация;
4) закрываемая собственником информация;
5) коммерческая тайна.

Вопрос 3. Кто может быть владельцем защищаемой информации?
1) только государство и его структуры;
2) предприятия акционерные общества, фирмы;
3) общественные организации;
4) только вышеперечисленные;
5) кто угодно.

Вопрос 4. Какие сведения на территории РФ могут составлять коммерческую тайну?
1) учредительные документы и устав предприятия;
2) сведенья о численности работающих, их заработной плате и условиях труда;
3) документы о платежеспособности, об уплате налогов, о финансово-хозяйственной деятельности;
4) другие;
5) любые.
Вопрос 5. Какой самый прямой и эффективный способ склонения к сотрудничеству?
1) психическое давление;
2) подкуп;
3) преследование;
4) шантаж;
5) угрозы.

Вопрос 6. Завершающим этапом любого сбора конфиденциальной информации является
1) копирование;
2) подделка;
3) аналитическая обработка;
4) фотографирование;

5) наблюдение.

Вопрос 7. Причины связанные с информационным обменом приносящие наибольшие убытки?
1) остановка или выход из строя информационных систем;
2) потери информации;
3) неискренность;
4) проникновение в информационную систему;
5) перехват информации.

Вопрос 8. Какие цели преследуются при активном вторжении в линии связи?
1) анализ информации (содержание сообщений, частоту их следования и факты прохождения, пароли, идентификаторы коды) и системно-структурный анализ;
2) воздействие на поток сообщений(модификация, удаление и посылка ложных сообщений) или восприпятствие передаче сообщений;
3) инициализация ложных соединений;
4) варианты 1 и 2;
5) варианты 2 и 3.

Вопрос 9. Что определяет модель нарушителя?
1) категории лиц, в числе которых может оказаться нарушитель;
2) возможные цели нарушителя и их градации по степени важности и опасности;
3) предположения о его квалификации и оценка его технической вооруженности;
4) ограничения и предположения о характере его действий;
5) все выше перечисленные.

Вопрос 10. Выберите наиболее полный список мотивов, которые преследуют компьютерные пираты (хакеры), пытаясь получить несанкционированный доступ к информационной системе или вычислительной сети.
1) ознакомление с информационной системой или вычислительной сетью;
2) похитить программу или иную информацию;
3) оставить записку, выполнить, уничтожить или изменить программу;
4) вариант 2 и 3;
5) вариант 1, 2 и 3.

Вопрос 11. К какому методу относятся следующие действия: имитация или искажение признаков и свойств отдельных элементов объектов защиты, создания ложных объектов?
1) скрытие;
2) дезинформация;
3) дробление;
4) кодирование;
5) шифрование.

Вопрос 12. Что в себя включают морально-нравственные методы защиты информации?
1) воспитание у сотрудника, допущенного к секретам, определенных качеств, взглядов и убеждений;
2) контроль работы сотрудников, допущенных к работе с секретной информацией;
3) обучение сотрудника, допущенного к секретам, правилам и методам защиты информации, и навыкам работы с ней;
4) вариант ответа 1 и 3;
5) вариант ответа 1, 2 и 3.

Вопрос 13. Что включают в себя технические мероприятия по защите информации?
1) поиск и уничтожение технических средств разведки;
2) кодирование информации или передаваемого сигнала;
3) подавление технических средств постановкой помехи;
4) применение детекторов лжи;
5) все вышеперечисленное.

Вопрос 14. Какие основные направления в защите персональных компьютеров от несанкционированное доступа Вы знаете?
1) недопущение нарушителя к вычислительной среде;
2) защита вычислительной среды;
3) использование специальных средств защиты информации ПК от несанкционированного доступа;
4) все вышеперечисленные;
5) правильного ответа нет.

Вопрос 15. Какие средства защиты информации в ПК наиболее распространены?
1) применение различных методов шифрования, не зависящих от контекста информации;
2) средства защиты от копирования коммерческих программных продуктов;
3) средства защиты вычислительных ресурсов, использующие парольную идентификацию и ограничивающие доступ несанкционированного пользователя;
4) защита от компьютерных вирусов и создание архивов;
5) все вышеперечисленные.

Вопрос № 16. На какие группы делятся информационные ресурсы государства?
1) информация открытая, информация запатентованная и информация, "закрываемая" ее собственником, владельцем и защищаемая им с помощью отработанных механизмов защиты государственной, коммерческой или другой охраняемой тайны
2) информация открытая и информация запатентованная
3) отработанных механизмов защиты государственной, коммерческой или другой охраняемой тайны

Вопрос № 17. Кто является собственником защищаемой информации?
1) юридическое лицо, которое по своему усмотрению владеет, пользуется и распоряжается принадлежащей ему информацией
2) юридическое или физическое лицо, которое по своему усмотрению владеет, пользуется и распоряжается принадлежащей ему информацией
3) физическое лицо, которое по своему усмотрению владеет, пользуется и распоряжается принадлежащей ему информацией

Вопрос № 18. Одной из проблем защиты информации является…
1) классификация возможных каналов утечки информации
2) ее разнообразие
3) ее доступность

Вопрос № 19. К каналам утечки относятся…
1) хищение носителей информации; чтение информации с экрана ПЭВМ посторонним лицом; чтение информации из оставленных без присмотра распечаток программ; подключение к устройствам ПЭВМ специальных аппаратных средств, обеспечивающих доступ к информации;
2) использование технических средств для перехвата электромагнитных излучений технических средств ПЭВМ; несанкционированный доступ программ к информации;

расшифровка программой зашифрованной информации; копирование программой информации с носителей.
3) все вышеперечисленное

Вопрос № 20. Известно, что информация - это сведения о…
1) предметах, объектах
2) явлениях и процессах, отображаемые в сознании человека или на каком-либо носителе, для последующего их восприятия человеком
3) все вышеперечисленное

Вопрос № 21. Информационная коммуникация предполагает…
1) обмен между субъектами отношений в виде совокупности процессов представления, передачи и получения информации
2) доступность информации и ее разнообразие
3) все вышеперечисленное
Вопрос № 22. Основные положения современной концепции защиты информации можно свести к следующим положениям:
1) защита информации в государстве должна обеспечить информационную безопасность личности, общества и государства
2) защита должна обеспечить охрану информационных ресурсов страны
3) все вышеперечисленное

Вопрос № 23. Особенности защиты персональных компьютеров (ПК) обусловлены…
1) спецификой их использования
2) частотой процессора
3) все вышеперечисленное

Вопрос № 24. Среди стандартных защитных средств персонального компьютера наибольшее распространение получили…
1) средства, использующие парольную идентификацию и методы шифрования; средства защиты от копирования программных продуктов; защита от компьютерных вирусов и создание архивов.
2) ограничение доступа к персональному компьютеру
3) все вышеперечисленное

Вопрос № 25. Вирусы условно подразделяются на классы по следующим признакам:
1) по среде обитания; по способу заражения; по возможностям
2) по среде обитания, по скорости распространения, по названию
3) по способу заражения, по названию

Примеры заданий для контрольной работы

1. Виды угроз информационной безопасности Российской Федерации?
2. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности?
3. Угрозы информационному обеспечению государственной политики Российской Федерации?
4. Угрозы развитию отечественной индустрии информации?
5. Угрозы безопасности информационных и телекоммуникационных средств и сис тем?
6. Источники угроз информационной безопасности Российской Федерации?
7. К внешним источникам информационной безопасности Российской Федерации относятся?

8. К внутренним источникам информационной безопасности Российской Федера ции относятся?
9. Угрозы информационной безопасности для автоматизированных систем обра ботки информации (АСОИ)?
10. Уязвимость основных структурно-функциональных элементов распределенных АСОИ?
11. Основные виды угроз безопасности субъектов информационных отношений?
12. Классификация угроз безопасности информации?
13. Естественные угрозы информации это?
14. Искусственные угрозы информации это?
15. Непреднамеренные угрозы информации это?
16. Преднамеренные угрозы информации это?
17. Основные непреднамеренные искусственные угрозы?
18. Основные преднамеренные искусственные угрозы?
19. классификация каналов проникновения в систему и утечки информации?
20. Неформальная модель нарушителя в АС?
21. Удаленные атаки на интрасети?
22. Что принято понимать под удаленной атакой?
23. Классификация удаленных атак?

2. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ

Лекции оцениваются по посещаемости, активности, умению выделить главную мысль.

Практические занятия оцениваются по самостоятельности выполнения работы, грамотности в оформлении, правильности выполнения.

Самостоятельная работа оценивается по качеству и количеству выполненных домашних или контрольных работ, грамотности в оформлении, правильности выполнения.

Промежуточная аттестация проводится в форме зачета и экзамена.

Для получения зачета и экзамена студент очной формы обучения должен в течение семестра активно посещать лекции и принимать участие в обсуждении вопросов, касающихся изучаемой темы, выполнить и защитить отчеты по практическим занятиям.

Для получения зачета и экзамена студент заочной формы обучения должен написать контрольную работу, активно посещать лекции и принимать участие в обсуждении вопросов, касающихся изучаемой темы, выполнить и защитить отчеты по практическим занятиям.

Критерии оценки зачета и экзамена могут быть получены в тестовой форме: количество баллов или удовлетворительно, хорошо, отлично. Для получения соответствующей оценки на зачете и экзамене по курсу используется накопительная система бально-рейтинговой работы студентов. Итоговая оценка складывается из суммы баллов или оценок, полученных по всем разделам курса и суммы баллов, полученной на зачете и экзамене.

Таблица 2.1 - Критерии оценки уровня знаний студентов с использованием теста на зачете и экзамене по учебной дисциплине

Оценка	Характеристики ответа студента
Отлично	86-100 % правильных ответов

Хорошо	71-85 %
Удовлетворительно	51- 70%
Неудовлетворительно	Менее 51 %

Оценка «зачтено» соответствует критериям оценок от «отлично» до «удовлетворительно».

Оценка «не зачтено» соответствует критерию оценки «не удовлетворительно».

Количество баллов и оценка неудовлетворительно, удовлетворительно, хорошо, отлично определяются программными средствами по количеству правильных ответов к количеству случайно выбранных вопросов.

Критерии оценивания компетенций, следующие:

1. Ответы имеют полные решения (с правильным ответом). Их содержание свидетельствует об уверенных знаниях обучающегося и о его умении решать профессиональные задачи, оценивается в 5 баллов (отлично);

2. Более 75% ответов имеют полные решения (с правильным ответом). Их содержание свидетельствует о достаточных знаниях обучающегося и его умении решать профессиональные задачи – 4 балла (хорошо);

3. Не менее 50% ответов имеют полные решения (с правильным ответом). Их содержание свидетельствует об удовлетворительных знаниях обучающегося и о его ограниченном умении решать профессиональные задачи, соответствующие его будущей квалификации – 3 балла (удовлетворительно);

4. Менее 50% ответов имеют решения с правильным ответом. Их содержание свидетельствует о слабых знаниях обучающегося и о его неумении решать профессиональные задачи – 2 балла (неудовлетворительно).