**КАЗАНСКИЙ КООПЕРАТИВНЫЙ ИНСТИТУТ (ФИЛИАЛ)
АВТОНОМНОЙ НЕКОММЕРЧЕСКОЙ ОБРАЗОВАТЕЛЬНОЙ
ОРГАНИЗАЦИИ ВЫСШЕГО ОБРАЗОВАНИЯ
ЦЕНТРОСОЮЗА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ УНИВЕРСИТЕТ КООПЕРАЦИИ»**

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

# ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

Специальность: 10.05.01 Компьютерная безопасность
Специализация: «Разработка защищенного программного обеспечения»
Формы обучения: очная
Объем дисциплины:
в зачетных единицах: 3 з.е.
в академических часах: 108 ак.ч.

Форма промежуточной аттестации: зачет

2025

Оценочные материалы по дисциплине **Основы построения защищенных компьютерных сетей**

**обсуждены и рекомендованы** к утверждению решением кафедры естественных дисциплин, сервиса и туризма от 25 марта 2025 г., протокол № 6

**одобрены** Научно-методическим советом Казанского кооперативного института (филиала) от 2 апреля 2025 г., протокол № 3

# СОДЕРЖАНИЕ

Целью оценочных материалов по дисциплине (модулю) (далее –ОМ) является комплексная оценка результатов обучения по дисциплине (модулю) *Основы построения защищенных компьютерных сетей* и установление уровня сформированности компетенций обучающегося.

ОМ предназначен для проведения текущего контроля успеваемости и промежуточной аттестации.

ОМ включает оценочные средства для проведения текущего контроля успеваемости и промежуточной аттестации.

Оценочные материалы разработаны в соответствии с рабочей программой дисциплины «*Основы построения защищенных компьютерных сетей»*.

## 1. Паспорт оценочных материалов по дисциплине «*Основы построения защищенных компьютерных сетей*»

| Формируемые компетенции (код и наименование компетенции) | Индикаторы достижения компетенций | Планируемые результаты обучения | Контролируемые разделы, темы дисциплины | Наименование оценочного средства[1] | |
|---|---|---|---|---|---|
| | | | | Текущий контроль | Промежуточная аттестация |
| 1 | 2 | 3 | 4 | 5 | 6 |
| ОПК-8 Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей | ОПК-8.1 Демонстрирует умение применять методику имитационного моделирования и инструментальные средства её поддержки при проведении исследований в области обеспечения безопасности компьютерных систем и сетей | Демонстрирует умение применять методику имитационного моделирования и инструментальные средства её поддержки при проведении исследований в области обеспечения безопасности компьютерных систем и сетей | Раздел 1. Основы информационной безопасности. Тема1. Общие проблемы безопасности. Основные положения теории информационной безопасности.<br><br>Тема2. Нормативно-правовые аспекты информационной безопасности и защиты информации. | *Рефераты, Тесты, Кейс-задание.* | *Контрольные тесты,экзамен* |
| | ОПК-8.2 Демонстрирует умение решать стандартные профессиональные | Демонстрирует умение решать стандартные профессиональные задачи с | Раздел2 Методические принципы формирования информационной безопасности. | *Тесты, рефераты* | *Контрольные тесты,экзамен.* |

| Формируемые компетенции (код и наименование компетенции) | Индикаторы достижения компетенций | Планируемые результаты обучения | Контролируемые разделы, темы дисциплины | Наименование оценочного средства[1] | |
|---|---|---|---|---|---|
| | | | | Текущий контроль | Промежуточная аттестация |
| 1 | 2 | 3 | 4 | 5 | 6 |
| | задачи с применением естественнонаучных и общеинженерных знаний, методов математического анализа и математического моделирования | применением естественнонаучных и общеинженерных знаний, методов математического анализа и математического моделирования | Тема3. Административно-организационные аспекты информационной безопасности и защиты информации.<br><br>Тема4. Методы защиты информации в современных информационных системах. | | |

## 2. Оценочные материалы по дисциплине *«Основы построения защищенных компьютерных сетей»*

### 2.1 Оценочные материалы для проведения текущего контроля успеваемости

Тематика рефератов

Тема 1 Общие проблемы безопасности. Основные положения теории информационной безопасности.

1. Понятийный аппарат и основы терминологии информационной и национальной безопасности.
2. Виды национальной безопасности и краткая характеристика.
3. Системные связи информационной безопасности с другими видами национальной безопасности.
4. Антропогенные информационные уязвимости с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
5. Техногенные информационные уязвимости.
6. Организационно-правовые и комбинированные информационные уязвимости.
7. Эндогенные и экзогенные, антропогенные и техногенные угрозы и информационной безопасности, их классификация.
8. Недостатки традиционного подхода к информационной безопасности с объектной точки зрения
9. Наиболее распространенные угрозы работы с информацией из различных источников, в том числе в глобальных компьютерных сетях
10. Основные определения и критерии классификации угроз на основе решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры

Тема 2 Нормативно-правовые аспекты информационной безопасности и защиты информации.

1. Угрозы конфиденциальности, целостности и доступности информации с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
2. Организационно-правовые средства обеспечения информационной безопасности, категорирование информации, допуски доступ к информационным ресурсам.
3. Роль стандартов и спецификаций с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
4. Наиболее важные стандарты и спецификации в области информационной безопасности
5. Критериев оценки безопасности информационных технологий "

(Evaluation Criteria for IT Security, ECITS).

6. "Общие критерии", часть 2. Функциональные требования безопасности

7. Федеральный стандарт США FIPS 140-2

8. Требования безопасности для криптографических модулей

9. Британский стандарт BS 7799

10.Спецификация Internet-сообщества "Как выбирать поставщика Интернет-услуг"

11.Спецификация Internet-сообщества "Как реагировать на нарушения информационной безопасности" с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

12. Спецификация Internet-сообщества "Руководство по информационной безопасности предприятия работать с информацией из различных источников, в том числе в глобальных компьютерных сетях

13. Спецификации Internet-сообщества IPsec

14. Основные понятия и идеи рекомендаций семейства X.500

Тема 3 Административно-организационные аспекты информационной безопасности и защиты информации.

1.Организационная защита информации с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

2. Работа с конфиденциальной информацией.

3. Функции службы безопасности.

Классификация способов защиты информации с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

4. Программа безопасности предприятия

5.Синхронизация программы безопасности с жизненным циклом систем с учетом работы с информацией из различных источников, в том числе в глобальных компьютерных сетях

6. Анализ угроз и их последствий, выявление уязвимых мест в защите

7. Процедурный уровень информационной безопасности

8. Реагирование на нарушения режима безопасности

9. Основные программно-технические меры программы безопасности предприятия

10. Основные понятия программно-технического уровня информационной безопасности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Тема 4. Методы защита информации в информационных системах.

1.Основные принципы организации процесса защиты информации

2. Угрозы информационной безопасности
3. Средства защиты информации с возможностью работать с информацией из различных источников, в том числе в глобальных компьютерных сетях.
4. Защита информации от утечки по техническим каналам.

5. Формирование оценки эффективности системы информационной безопасности.
6. Особенности современных информационных систем, существенные с точки зрения безопасности.
7. Архитектурная безопасность информационной системы.
8. Идентификация и аутентификация, управление доступом.
9. Парольная аутентификация, работа в глобальных компьютерных сетях.
10. Сервер аутентификации Kerberos
11. Идентификация/ аутентификация с помощью биометрических данных.

Критерии оценки выполнения реферата по учебной дисциплине

Оценка «отлично» выставляется студенту, если тема реферата раскрыта в полной мере и все требования по написанию реферата соблюдены.

Оценка «хорошо» выставляется студенту, если недостаточно раскрыта тема реферата, но все требования по написанию реферата соблюдены.

Оценка «удовлетворительно» выставляется студенту, если недостаточно раскрыта тема реферата, не все требования по написанию реферата соблюдены, присутствуют ошибки и неточности в работе.

Оценка «неудовлетворительно» выставляется студенту, если отсутствует реферат.

| **Оценка** | **Критерии** |
|---|---|
| «Отлично» | Оценка «отлично» выставляется студенту, если тема реферата раскрыта в полной мере и все требования по написанию реферата соблюдены |
| «Хорошо» | Оценка «хорошо» выставляется студенту, если недостаточно раскрыта тема реферата, но все требования по написанию реферата соблюдены. |
| «Удовлетворительно» | Оценка «удовлетворительно» выставляется студенту, если недостаточно раскрыта тема реферата, не все требования по написанию реферата соблюдены, присутствуют ошибки и неточности в работе. |

| | |
|---|---|
| «Неудовлетворительно» | Оценка «неудовлетворительно» выставляется студенту, если отсутствует реферат. |

## ТИПОВЫЕ ТЕСТЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ

Раздел 1. Основы информационной безопасности

Тема 1 Общие проблемы безопасности. Основные положения теории информационной безопасности

вопрос 1

Искать, получать, передавать, производить и распространять информацию любым законным способом имеет

1. совершеннолетний
2. каждый
3. только гражданин РФ

вопрос 2

На чем основан принцип работы антивирусных мониторов?

1. На перехватывании вирусоопасных ситуаций и сообщении об этом пользователю

2. На проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются маски

3. На подсчете контрольных сумм для присутствующих на диске файлов или системных секторов. Эти суммы затем сохраняются в базе данных антивируса, а также другая информация: длина файлов, дата их последней модификации и т.д.

вопрос3

На чем основан принцип работы антивирусных иммунизаторов?

1. На защите системы от поражения вирусом какого-то определенного вида. Файлы на дисках модифицируются таким образом, что вирус принимает их за уже зараженные

2. На проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются маски

3. На подсчете контрольных сумм для присутствующих на диске файлов или системных секторов. Эти суммы затем сохраняются в базе данных антивируса, а также другая информация: длина файлов, дата их последней модификации и т.д.

вопрос 4

Что необходимо сделать при обнаружении файлового вируса?

1. Компьютер необходимо отключить от сети и проинформировать системного администратора

2. Компьютер от сети отключать не следует, так как вирусы этого типа по сети не распространяются

3. Вместо отключения компьютера от сети достаточно на период лечения убедиться в том, что соответствующий редактор неактивен

вопрос 5

Что необходимо сделать при обнаружении загрузочного вируса?

1. Компьютер необходимо отключить от сети и проинформировать системного администратора

2. Компьютер от сети отключать не следует, так как вирусы этого типа по сети не распространяются

3. Вместо отключения компьютера от сети достаточно на период лечения убедиться в том, что соответствующий редактор неактивен

вопрос 6

Что необходимо сделать при обнаружении макровируса?

1. Вместо отключения компьютера от сети достаточно на период лечения убедиться в том, что соответствующий редактор неактивен

2. Компьютер необходимо отключить от сети и проинформиравать системного администратора

3. Компьютер от сети отключать не следует, так как вирусы этого типа по сети не распространяются

вопрос 7

В чем заключается метод защиты - ограничение доступа?

1. В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям

2. В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями

3. В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы

вопрос8

В чем заключается метод защиты информации - разграничение доступа?

1. В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям

2. В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями

3. В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы

вопрос 9

В чем заключается метод защиты информации - разделение доступа (привелегий)

1. В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы

2. В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям

3. В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями

вопрос 10

Что означает термин БЕЗОПАСНОСТЬ ИНФОРМАЦИИ

1. Потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному её тиражированию.

2. Свойство системы, в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.

3. Защищенность информации от нежелательного её разглашения, искажения, утраты или снижения степени доступности информации, а также незаконного её тиражирования

Тема 2 Нормативно-правовые аспекты информационной безопасности и защиты информации.

вопрос 1

Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?

1. Поддержка
2. Выполнение анализа рисков
3. Определение цели и границ.
4.. Делегирование полномочий

вопрос 2

Что означает термин ПРАВОВЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ?

1. Это действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения.

2. Это традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией.

3. Это меры, регламентирующие процессы функционирования системы обработки данных, использования её ресурсов.

вопрос3

Что означает термин МОРАЛЬНО-ЭТИЧЕСКИЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ?

1. Это традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией.

2. Это действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения.

3. Это меры, регламентирующие процессы функционирования системы обработки данных, использование её ресурсов.

вопрос 4

Что означает термин ОРГАНИЗАЦИОННЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ?

1. Это меры, регламентирующие процессы функционирования системы обработки данных, использование её ресурсов, деятельность персонала, а так же порядок взаимодействия пользователей с системой.

2. Это действующие в стране законы, указы и другие нормативные акты.

3. Это традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией.

вопрос 5

Что означает термин ФИЗИЧЕСКИЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ?

1. Это разного рода механические или электронно-механические устройства и сооружения, специально предназначенные для создания различных препятствий на возможных путях проникновения доступа потенциальных нарушителей к компонентам защищаемой информации.

2. Это действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения.

3. Это меры, регламентирующие процессы функционирования системы обработки данных, использование её ресурсов.

вопрос 6

Что означает термин АУТЕНТИФИКАЦИЯ?

1. Это проверка целостности информации, программы, документа
2. Это проверка подлинности объекта или субъекта
3. Это присвоение имени субъекту или объекту

вопрос 7

Что означает термин ВЕРИФИКАЦИЯ?

1. Это присвоение имени субъекту или объекту.
2. Это проверка подлинности субъекта или объекта.
3. Это проверка целостности информации, программы, документа.

вопрос8

Что означает термин ИДЕНТИФИКАЦИЯ?

1. Это присвоение имени субъекту или объекту.
2. Это проверка подлинности субъекта или объекта.
3. Это проверка целостности информации, программы, документа.

вопрос 9

Что означает термин КРИПТОГРАФИЯ?

1. Это преобразование информации в виде условных сигналов с целью автоматизации её хранения, обработки, передачи и ввода-вывода
2. Это метод специального преобразования информации с целью сокрытия от посторонних лиц
3. Это преобразование информации при её передаче по каналам связи от одного элемента вычислительной сети к другому

вопрос 10

Что означает термин КОДИРОВАНИЕ ИНФОРМАЦИИ?

1. Это преобразование информации в виде условных сигналов с целью автоматизации её хранения, обработки, передачи и ввода-вывода.
2. Это метод специального преобразования информации с целью сокрытия от посторонних лиц.
3. Это криптографическое преобразование информации при её передаче по каналам связи от одного элемента в вычислительной сети к другому.

Раздел 2. Методические принципы формирования информационной безопасности

Тема 3 Административно-организационные аспекты информационной безопасности и защиты информации.

Вопрос 1

Собственником информации не может быть:

а) государство;

б) юридическое лицо;

в) группа физических лиц;

г) физическое лицо;
д) ответы а – г правильны;
е) нет правильного ответа.

Вопрос 2.
Терминология в сфере защиты информации регулируется
а) ГОСТ Р 6.30 – 2003
б) ГОСТ 51141 – 98
в) ГОСТ 50922 – 96
г) Гражданским кодексом.

Вопрос 3.
Заранее намеченный результат защиты информации – это
а) замысел защиты информации;
б) цель защиты информации;
в) уровень эффективности защиты информации.

Вопрос 4.
Содержание и порядок действий, направленных на обеспечение защиты информации – это:
а) мероприятие по защите информации;
б) система защиты информации
в) организация защиты информации.

Вопрос 5.
Субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и (или) собственником информации – это
а) носитель информации
б) собственник информации
в) владелец информации
г) пользователь информации

Вопрос 6.
В настоящее время по степени конфиденциальности можно классифицировать информацию:
а) составляющую коммерческую тайну;
б) составляющую государственную тайну; в) составляющую служебную тайну;
г) составляющую профессиональную тайну.

Вопрос 7.
В каких областях деятельности может быть государственная тайна
а) военной
б) образовательной

в) экономической
г) контрразведывательной
д) внешнеполитической
е) внутриполитической
ж) разведывательной
з) оперативно-розыскной
и) экологической
к) правильны все ответы.

Вопрос 8.

Классифицированный список типовой и конкретной ценной информации о выполняемых работах, производимой продукции, научных и деловых идеях, технологических новшествах – это

а) перечень ценных и конфиденциальных документов организации
б) перечень конфиденциальных сведений организации
в) перечень типовых документов, образующихся в деятельности организации.

Вопрос 9.

Организацией конфиденциального делопроизводства непосредственно занимаются:

а) все сотрудники организации в меру своих сил и обязанностей
б) служба безопасности
в) сектор конфиденциального делопроизводства в составе службы безопасности
г) первый руководитель организации
д) постоянно действующая экспертная комиссия
е) комиссии по проверке наличия, состояния и учета документов

Тема 4. Методы защита информации в информационных системах.

Вопрос 1.

Кто имеет право давать разрешение на ознакомление со всеми видами конфиденциальных документов организации всем категориям сотрудников и другим лицам?

а) руководитель службы безопасности
б) первый руководитель организации
в) руководитель сектора конфиденциального делопроизводства в составе службы безопасности
г) правильны все варианты

Вопрос 2.

Для работы сотруднику подразделения понадобились конфиденциальные сведения и документы другого подразделения. Кто должен дать разрешение на ознакомление со сведениями и документами?

а) непосредственный начальник этого сотрудника

б) заместитель руководителя организации, курирующий данное направление

в) начальник подразделения, содержащего необходимые конфиденциальные сведения и документы

г) только первый руководитель организации.

Вопрос 3.

Конфиденциальные документы уничтожаются, если

а) они являются исполненными

б) истек срок их конфиденциальности

в) истек срок их хранения

Вопрос 4.

Отправка нешифрованного конфиденциального документа по факсу

а) не допускается

б) допускается

в) допускается, если на документе стоит гриф конфиденциальности

Вопрос 5.

При проверках наличия конфиденциальных документов:

а) проверяют только документы, не трогая дела и иные носители конфиденциальной информации, т.к. в противном случае проверки будут очень громоздкими и долговременными

б) проверяют документы и дела, не трогая иные носители конфиденциальной информации, т.к. все, что связано с компьютерными технологиями, будет проверено специалистами по компьютерной безопасности

в) проверяют документы и дела, а также иные носители конфиденциальной информации

Критерии оценивания тестовых заданий для текущего контроля

| **Оценка** | **Критерии** |
|---|---|
| «Отлично» | оценка «отлично» (5 баллов) выставляется при условии правильного ответа студента не менее чем на 85% контрольных заданий |
| «Хорошо» | оценка «хорошо» (4 балла) выставляется при условии правильного ответа студента не менее чем на 70% контрольных заданий |
| «Удовлетворительно» | оценка «удовлетворительно» (3 балла) выставляется при условии правильного ответа студента не менее чем на 51% контрольных заданий |

| | |
|---|---|
| «Неудовлетворительно» | оценка «неудовлетворительно» (1-2 балла) выставляется при условии правильного ответа студента менее чем на 50% контрольных заданий |

## ТИПОВОЕ КЕЙС-ЗАДАНИЕ ПО ДИСЦИПЛИНЕ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

### Построение информационной безопасности предприятия

Цель: знакомство с основными принципами построения концепции ИБ предприятия, с учетом особенностей его информационной инфраструктуры.

ГОСТ Р ИСО/МЭК 15408 ГОСТ Р ИСО/МЭК 27000 ГОСТ Р ИСО/МЭК 17799, ISO 27001/17799

Краткие теоретические сведения

Концепция ИБ в общих чертах определяет, что необходимо сделать для защиты информации. Политика ИБ детализирует положения Концепции, и говорит как, какими средствами и способами они должны быть реализованы. Концепция информационной безопасности используется для:

- принятия обоснованных управленческих решений по разработке мер защиты информации;
- выработки комплекса организационно-технических и технологических мероприятий по выявлению угроз информационной безопасности и предотвращению последствий их реализации;
- координации деятельности подразделений по созданию, развитию и эксплуатации информационной системы с соблюдением требований обеспечения безопасности информации;
- для формирования и реализации единой политики в области обеспечения информационной безопасности.

Задание. Разработать концепцию информационной безопасности компании по следующему примерному плану

1. Цели системы информационной безопасности
2. Задачи системы информационной безопасности.
3. Объекты информационной безопасности.
4. Вероятные нарушители.
5. Основные виды угроз информационной безопасности.
6. Классификация угроз.
    a. Основные непреднамеренные искусственные угрозы.
    b. Основные преднамеренные искусственные угрозы.
7. Мероприятия по обеспечению информационной безопасности.

8. Средства защиты от потенциальных угроз.

Разработайте вариант политики паролей

Предложите ПО для антивирусной защиты (проведя сравнительный анализ цен, возможностей и пр)

Варианты заданий

1. Поликлиника
2. Офис страховой компании
3. Офис адвоката
4. Гостиница
5. Компания по разработке ПО для сторонних организаций
6. Интернет-магазин

1. Законодательство РФ в области информационной безопасности

Цель занятия – закрепление теоретических знаний в области правового обеспечения информационной безопасности.

1. вопросы для обсуждения

1. Конституция Российской Федерации, Доктрина информационной безопасности Российской Федерации.

2. Федеральные законы в области информации и информационной безопасности.

3. Указы президента РФ и постановления правительства РФ в области информации и информационной безопасности.

4. Правовые режимы защиты информации.

5. Правовые вопросы защиты информации с использованием технических средств.

6. В чем заключается двуединство документированной информации с правовой точки зрения.

Критерии оценки при выполнении кейс-задания.

| **Оценка** | **Критерии** |
|---|---|
| «Отлично» | Задание решено самостоятельно. При этом составлен правильный алгоритм решения задания, в логических рассуждениях, в выборе формул и решении нет ошибок, получен верный ответ, задание решено рациональным способом. |
| «Хорошо» | Задание решено с помощью преподавателя. Составлен правильный алгоритм решения задания, в логическом рассуждении и решении нет существенных ошибок; правильно сделан выбор формул для решения; есть объяснение решения, но задание решено нерациональным способом или допущено не более двух несущественных ошибок, получен верный ответ. |
| «Удовлетворительно» | Задание решено с подсказками преподавателя. Задание понято правильно, в логическом рассуждении нет существенных |

| | |
|---|---|
| | ошибок, но допущены существенные ошибки в выборе формул или в математических расчетах; задание решено не полностью или в общем виде. |
| «Неудовлетворительно» | Задание не решено. |

## 2.2 Оценочные материалы для проведения промежуточной аттестации

Вопросы к экзамену

1. Роль современного информационного пространства в обеспечении информационной безопасности организации.
2. Терминология в сфере защиты документированной информации.
3. Генеральный регламент и общее учреждение министерств по вопросам защиты информации.
4. Системные связи информационной безопасности с другими видами национальной безопасности.
5. Антропогенные информационные уязвимости с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
6. Техногенные информационные уязвимости.
7. Организационно-правовые и комбинированные информационные уязвимости.
8. Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, их классификация.
9. Недостатки традиционного подхода к информационной безопасности с объектной точки зрения
10. Наиболее распространенные угрозы работы с информацией из различных источников, в том числе в глобальных компьютерных сетях
11. Основные определения и критерии классификации угроз на основе решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры
12. Шифрование информации в России: исторический аспект.
13. Становление системы информации ограниченного доступа.
14. Возникновение и развитие информационного права, его место в системе российского права.
15. Государственная тайна в истории России.
16. Доктрина информационной безопасности РФ.
17. Общая характеристика законодательства РФ о коммерческой тайне.
18. Разновидности служебной и профессиональной тайн (налоговая, банковская, нотариальная, врачебная и др.).
19. Трудовое законодательство о защите конфиденциальной информации.

20. Ответственность за разглашение конфиденциальной информации и государственной тайны.

21. Угрозы информационной безопасности организации: виды, способы предупреждения.

22. Организационные документы в системе защиты конфиденциальной информации.

23. Методология разработки перечней конфиденциальных сведений и документов.

24. Организация защиты информации в системе менеджмента качества (стандарты ИСО серии 9000).

25. Защита конфиденциальной информации в процессе подготовки проектов документов.

26. Защита конфиденциальной информации в ходе совещаний и переговоров.

27. Особенности подготовки к сдаче в архив конфиденциальных документов.

28. Организация системы доступа сотрудников к конфиденциальным документам.

29. Технические требования к хранению конфиденциальных документов.

30. Технические требования к использованию конфиденциальных документов

31. Законодательные нормы о предоставлении конфиденциальной информации негосударственными организациями.

32. Законодательные нормы о предоставлении конфиденциальной информации органами государственной власти и местного самоуправления.

33. Процедура обыска, ее документирование.

34. Организационная защита информации с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

35. Работа с конфиденциальной информацией.

36. Функции службы безопасности.

37. Классификация способов защиты информации с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

38. Программа безопасности предприятия

39. Синхронизация программы безопасности с жизненным циклом систем с учетом работы с информацией из различных источников, в том числе в глобальных компьютерных сетях

40. Анализ угроз и их последствий, выявление уязвимых мест в защите

41. Процедурный уровень информационной безопасности

42. Реагирование на нарушения режима безопасности

43. Основные программно-технические меры программы безопасности предприятия

44. Основные понятия программно-технического уровня

информационной безопасности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

## Критерии оценки для проведения экзамена по дисциплине (ответы на вопросы)

Шкала оценивания результатов промежуточной аттестации и критерии выставления оценок.

| Оценка | Уровень сформированности компетенции | Критерии |
|---|---|---|
| «Отлично» («зачтено») | Высокий | Обучающийся глубоко и прочно усвоил весь программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагает, тесно увязывает теорию с практикой. Обучающийся не затрудняется с ответом при видоизменении задания, свободно справляется с практическими заданиями, показывает знания нормативного материала, правильно обосновывает принятые решения, владеет разносторонними навыками и приемами выполнения практических заданий, демонстрирует умение самостоятельно обобщать и излагать материал, не допуская ошибок |
| «Хорошо» («зачтено») | Хороший | Обучающийся твердо знает программный материал, грамотно и по существу излагает его, допускает несущественные неточности в ответе на вопросы, может правильно применять теоретические положения и владеет необходимыми навыками при выполнении практических заданий. |
| «Удовлетворительно» («зачтено») | Достаточный | Обучающийся усвоил только основной материал, но не знает отдельных деталей, допускает неточности и ошибки в ответе на вопросы, нарушает последовательность в изложении программного материала и испытывает затруднения при выполнении практических заданий. |
| «Неудовлетворительно» («не зачтено») | Недостаточный | Обучающийся не знает значительной части программного материала, допускает существенные ошибки, с большими затруднениями выполняет практические задания или выполняет неправильно. |

# ТИПОВЫЕ ТЕСТЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

вопрос 1

Искать, получать, передавать, производить и распространять информацию любым законным способом имеет

4. совершеннолетний
5. каждый
6. только гражданин РФ

вопрос 2

На чем основан принцип работы антивирусных мониторов?

4. На перехватывании вирусоопасных ситуаций и сообщении об этом пользователю

5. На проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются маски

6. На подсчете контрольных сумм для присутствующих на диске файлов или системных секторов. Эти суммы затем сохраняются в базе данных антивируса, а также другая информация: длина файлов, дата их последней модификации и т.д.

вопрос3

На чем основан принцип работы антивирусныхиммунизаторов?

4. На защите системы от поражения вирусом какого-то определенного вида. Файлы на дисках модифицируются таким образом, что вирус принимает их за уже зараженные

5. На проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются маски

6. На подсчете контрольных сумм для присутствующих на диске файлов или системных секторов. Эти суммы затем сохраняются в базе данных антивируса, а также другая информация: длина файлов, дата их последней модификации и т.д.

вопрос 4

Что необходимо сделать при обнаружении файлового вируса?

4. Компьютер необходимо отключить от сети и проинформировать системного администратора

5. Компьютер от сети отключать не следует, так как вирусы этого типа по сети не распространяются

6. Вместо отключения компьютера от сети достаточно на период лечения убедиться в том, что соответствующий редактор неактивен

вопрос 5

Что необходимо сделать при обнаружении загрузочного вируса?

4. Компьютер необходимо отключить от сети и проинформировать системного администратора

5. Компьютер от сети отключать не следует, так как вирусы этого типа по сети не распространяются

6. Вместо отключения компьютера от сети достаточно на период лечения убедиться в том, что соответствующий редактор неактивен

вопрос 6

Что необходимо сделать при обнаружении макровируса?

4. Вместо отключения компьютера от сети достаточно на период лечения убедиться в том, что соответствующий редактор неактивен

5. Компьютер необходимо отключить от сети и проинформиравать системного администратора

6. Компьютер от сети отключать не следует, так как вирусы этого типа по сети не распространяются

вопрос 7

В чем заключается метод защиты - ограничение доступа?

4. В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям

5. В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями

6. В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы

вопрос8

В чем заключается метод защиты информации - разграничение доступа?

4. В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям

5. В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями

6. В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы

вопрос 9

В чем заключается метод защиты информации - разделение доступа (привелегий)

4. В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы

5. В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям

6. В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями

вопрос 10

Что означает термин БЕЗОПАСНОСТЬ ИНФОРМАЦИИ

4. Потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному её тиражированию.

5. Свойство системы, в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.

6. Защищенность информации от нежелательного её разглашения, искажения, утраты или снижения степени доступности информации, а также незаконного её тиражирования

вопрос 11

Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?

1. Поддержка
2. Выполнение анализа рисков
3. Определение цели и границ.
4.. Делегирование полномочий

вопрос 12

Что означает термин ПРАВОВЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ?

1. Это действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения.

2. Это традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией.

3. Это меры, регламентирующие процессы функционирования системы обработки данных, использования её ресурсов.

Вопрос13

Что означает термин МОРАЛЬНО-ЭТИЧЕСКИЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ?

1. Это традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией.
2. Это действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения.
3. Это меры, регламентирующие процессы функционирования системы обработки данных, использование её ресурсов.

вопрос 14

Что означает термин ОРГАНИЗАЦИОННЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ?

1. Это меры, регламентирующие процессы функционирования системы обработки данных, использование её ресурсов, деятельность персонала, а так же порядок взаимодействия пользователей с системой.
2. Это действующие в стране законы, указы и другие нормативные акты.
3. Это традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией.

вопрос 15

Что означает термин ФИЗИЧЕСКИЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ?

1. Это разного рода механические или электронно-механические устройства и сооружения, специально предназначенные для создания различных препятствий на возможных путях проникновения доступа потенциальных нарушителей к компонентам защищаемой информации.
2. Это действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения.
3. Это меры, регламентирующие процессы функционирования системы обработки данных, использование её ресурсов.

вопрос 16

Что означает термин АУТЕНТИФИКАЦИЯ?

1. Это проверка целостности информации, программы, документа
2. Это проверка подлинности объекта или субъекта
3. Это присвоение имени субъекту или объекту

вопрос 17

Что означает термин ВЕРИФИКАЦИЯ?

1. Это присвоение имени субъекту или объекту.
2. Это проверка подлинности субъекта или объекта.

3. Это проверка целостности информации, программы, документа.

Вопрос18

Что означает термин ИДЕНТИФИКАЦИЯ?

1. Это присвоение имени субъекту или объекту.
2. Это проверка подлинности субъекта или объекта.
3. Это проверка целостности информации, программы, документа.

вопрос 19

Что означает термин КРИПТОГРАФИЯ?

1. Это преобразование информации в виде условных сигналов с целью автоматизации её хранения, обработки, передачи и ввода-вывода
2. Это метод специального преобразования информации с целью сокрытия от посторонних лиц
3. Это преобразование информации при её передаче по каналам связи от одного элемента вычислительной сети к другому

вопрос 20

Что означает термин КОДИРОВАНИЕ ИНФОРМАЦИИ?

1. Это преобразование информации в виде условных сигналов с целью автоматизации её хранения, обработки, передачи и ввода-вывода.
2. Это метод специального преобразования информации с целью сокрытия от посторонних лиц.
3. Это криптографическое преобразование информации при её передаче по каналам связи от одного элемента в вычислительной сети к другому.

вопрос 21

Собственником информации не может быть:

а) государство;
б) юридическое лицо;
в) группа физических лиц;
г) физическое лицо;
д) ответы а – г правильны;
е) нет правильного ответа.

вопрос 22.

Терминология в сфере защиты информации регулируется

а) ГОСТ Р 6.30 – 2003
б) ГОСТ 51141 – 98
в) ГОСТ 50922 – 96
г) Гражданским кодексом.

вопрос 23.

Заранее намеченный результат защиты информации – это

а) замысел защиты информации;

б) цель защиты информации;
в) уровень эффективности защиты информации.

вопрос 24.
Содержание и порядок действий, направленных на обеспечение защиты информации – это:
а) мероприятие по защите информации;
б) система защиты информации
в) организация защиты информации.

вопрос 25.
Субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и (или) собственником информации – это
а) носитель информации
б) собственник информации
в) владелец информации
г) пользователь информации

вопрос 26.
В настоящее время по степени конфиденциальности можно классифицировать информацию:
а) составляющую коммерческую тайну;
б) составляющую государственную тайну; в) составляющую служебную тайну;
г) составляющую профессиональную тайну.

вопрос 27.
В каких областях деятельности может быть государственная тайна
а) военной
б) образовательной
в) экономической
г) контрразведывательной
д) внешнеполитической
е) внутриполитической
ж) разведывательной
з) оперативно-розыскной
и) экологической
к) правильны все ответы.

вопрос 28.
Классифицированный список типовой и конкретной ценной информации о выполняемых работах, производимой продукции, научных и деловых идеях, технологических новшествах – это
а) перечень ценных и конфиденциальных документов организации

б) перечень конфиденциальных сведений организации

в) перечень типовых документов, образующихся в деятельности организации.

вопрос 29.

Организацией конфиденциального делопроизводства непосредственно занимаются:

а) все сотрудники организации в меру своих сил и обязанностей

б) служба безопасности

в) сектор конфиденциального делопроизводства в составе службы безопасности

г) первый руководитель организации

д) постоянно действующая экспертная комиссия

е) комиссии по проверке наличия, состояния и учета документов

вопрос 30.

Кто имеет право давать разрешение на ознакомление со всеми видами конфиденциальных документов организации всем категориям сотрудников и другим лицам?

а) руководитель службы безопасности

б) первый руководитель организации

в) руководитель сектора конфиденциального делопроизводства в составе службы безопасности

г) правильны все варианты

вопрос 31.

Для работы сотруднику подразделения понадобились конфиденциальные сведения и документы другого подразделения. Кто должен дать разрешение на ознакомление со сведениями и документами?

а) непосредственный начальник этого сотрудника

б) заместитель руководителя организации, курирующий данное направление

в) начальник подразделения, содержащего необходимые конфиденциальные сведения и документы

г) только первый руководитель организации.

вопрос 32.

Конфиденциальные документы уничтожаются, если

а) они являются исполненными

б) истек срок их конфиденциальности

в) истек срок их хранения

вопрос 33.

Отправка нешифрованного конфиденциального документа по факсу

а) не допускается

б) допускается

в) допускается, если на документе стоит гриф конфиденциальности

вопрос 34.

При проверках наличия конфиденциальных документов:

а) проверяют только документы, не трогая дела и иные носители конфиденциальной информации, т.к. в противном случае проверки будут очень громоздкими и долговременными

б) проверяют документы и дела, не трогая иные носители конфиденциальной информации, т.к. все, что связано с компьютерными технологиями, будет проверено специалистами по компьютерной безопасности

в) проверяют документы и дела, а также иные носители конфиденциальной информации

## Критерии оценки для проведения тестирования по дисциплине

Шкала оценивания результатов промежуточной аттестации и критерии выставления оценок.

| **Оценка** | **Уровень сформированности компетенции** | **Критерии** |
|---|---|---|
| «Отлично» («зачтено») | Высокий | Выполнено более 80% заданий предложенного теста |
| «Хорошо» («зачтено») | Хороший | Выполнено 60-80% заданий предложенного теста |
| «Удовлетворительно» («зачтено») | Достаточный | Выполнено 35-60% заданий предложенного теста |
| «Неудовлетворительно» («не зачтено») | Недостаточный | Выполнено менее 35% заданий предложенного теста |

**Обновление оценочных материалов дисциплины**

**обсуждено и рекомендовано к утверждению** решением кафедры
от _____ 20____ г., протокол № __ ___

**одобрено** Научно-методическим советом от _____ г., протокол №____