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

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ В КОМПЬЮТЕРНЫХ СИСТЕМАХ И СЕТЯХ

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 «Компьютерные преступления в компьютерных системах и сетях»

обсуждены и рекомендованы к утверждению решением кафедры гуманитарных дисциплин и иностранных языков от 21 марта 2025 г., протокол № 7

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 «Компьютерные преступления в компьютерных системах и сетях» и установление уровня сформированности компетенций обучающегося.

ОМ предназначены для проведения текущего контроля успеваемости и промежуточной аттестации.

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

Оценочные материалы разработаны в соответствии с рабочей программой дисциплины «Компьютерные преступления в компьютерных системах и сетях».

1. Паспорт оценочных материалов по дисциплине «Компьютерные преступления в компьютерных системах и сетях»

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
ПК-3.3 Способен участвовать в проведении экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов	ПК-3.3 Способен участвовать в проведении экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов	Знать: методы анализа защищенности компьютерных систем и сетей с использованием сканеров безопасности с целью противодействия компьютерным преступлениям, осуществляемым с использованием вредоносного программного обеспечения Уметь: реализовывать анализ защищенности сетевых сервисов автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей Владеть: навыками структуризации аналитической информации для составления отчётов по результатам проверок качества противодействия информационным атакам и операциям, реализуемым в компьютерных системах и сетях	Тема 1. Основы компьютерных преступлений Тема 2. Расследование компьютерных преступлений Тема 3. Противодействие компьютерным преступлениям, осуществляемым с использованием вредоносного программного обеспечения Тема 4. Противодействие компьютерным преступлениям, реализуемым в ходе проведения компьютерных сетевых атак Тема 5. Противодействие компьютерным преступлениям путем реализации политики безопасности	Реферат (темы 1-9) Тест № 1	Лабораторная работа 1-4
ПК-3.6 Способен участвовать в работах по	ПК-3.6 Способен участвовать в работах по	Знать: технологии поискаи анализа следов компьютерных преступлений, правонарушений и инцидентов	Тема 6. Преступления в сфере компьютерной информации	Реферат (темы 1-9) Тест № 2	Лабораторная работа 5-9

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
противодействию информационным атакам и операциям, реализуемым в компьютерных системах и сетях	противодействию информационным атакам и операциям, реализуемым в компьютерных системах и сетях	Уметь: применять методы и средства прогнозирования возможных путей развития новых видов компьютерных преступлений Владеть: навыками выявления индивидуальных признаков программы, позволяющих впоследствии идентифицировать ее автора, а также взаимосвязи с информационным обеспечением исследуемой компьютерной системы с информационным обеспечением исследуемой компьютерной системы	Тема 7. Компьютерные преступления, направленные на воздействие на критическую информационную инфраструктуру РФ Тема 8. Судебная практика по компьютерным преступлениям Тема 9. Предотвращение компьютерных преступлений		

Оценочные материалы по дисциплине «КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ В КОМПЬЮТЕРНЫХ СИСТЕМАХ И СЕТЯХ»

2.1 Оценочные материалы для проведения текущего контроля успеваемости

Тематика рефератов по темам 1-9

1. Понятие и виды вредной информации.
2. Правовые проблемы борьбы со «спамом»
3. Классификация вредоносных программ и защита от их воздействия.
4. Информационная война.
5. Информационное оружие.
6. Кибертерроризм как новая угроза информационной безопасности.
7. Виды угроз компьютерной безопасности.
8. Электронные деньги: проблемы правового регулирования
9. Правовое регулирование информационных технологий в области электронной коммерции
10. Правовое регулирование информационных технологий в области рекламы и маркетинга в Интернет
11. Правовое регулирование информационных технологий в области электронных банковских услуг
12. Правовое регулирование информационных технологий в области электронного документооборота
13. Стандартизация, сертификация и лицензирование в информационной сфере.
14. Информационные риски.
15. Стандартизация, сертификация и лицензирование в информационной сфере
16. Правовая защита объектов интеллектуальной собственности в информационной сфере.
17. Организационно-правовые проблемы международной информационной безопасности.
18. Юридическая ответственность информационных посредников за нарушение интеллектуальных прав в сети Интернет.
19. Ответственность должностных лиц за нарушения права граждан на доступ к информации о деятельности государственных органов.
20. Проблемы привлечения к уголовной ответственности при осуществлении экстремистской деятельности в сети Интернет.
21. Ограничение доступа к сайтам в сети «Интернет» с информацией, распространяемой с нарушением законодательства РФ.
22. Правовое регулирование информационных отношений в сфере документирования и документооборота в электронной форме.
23. Правовое регулирование использования электронной подписи.
24. Правовые основы информационной безопасности несовершеннолетних.

Критерии оценки выполнения рефератов 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.

Рекомендации по написанию реферата:

Реферат — письменная работа, выполняемая обучающимся в течение определенного срока.

Реферат — краткое точное изложение сущности какого-либо вопроса, темы на основе одной или нескольких книг, монографий или других первоисточников. Реферат должен содержать основные фактические сведения и выводы по рассматриваемому вопросу.

Реферат отвечает на вопрос — что содержится в данной публикации (публикациях). Реферат — не механический пересказ работы, а изложение ее существа.

Кроме реферирования прочитанной литературы, от обучающегося требуется аргументированное изложение собственных мыслей по рассматриваемому вопросу. Тему реферата предлагает преподаватель или сам обучающийся, в последнем случае она должна быть согласованна с преподавателем.

В реферате нужны развернутые аргументы, рассуждения, сравнения. Материал подается не столько в развитии, сколько в форме констатации или описания.

Содержание реферируемого произведения излагается объективно от имени автора. Если в первичном документе главная мысль сформулирована недостаточно четко, в реферате она должна быть конкретизирована и выделена.

Структура реферата:

1. Титульный лист.

2. После титульного листа на отдельной странице следует оглавление (план, содержание), в котором указаны названия всех разделов (пунктов плана) реферата и номера страниц, указывающие начало этих разделов в тексте реферата.

3. После оглавления следует введение. Объем введения составляет 1,5-2 страницы.

4. Основная часть реферата может иметь одну или несколько глав, состоящих из 2-3 параграфов (подпунктов, разделов) и предполагает осмысленное и логичное изложение главных положений и идей, содержащихся в изученной литературе. В тексте обязательны ссылки на первоисточники. В том случае если цитируется или используется чья-либо неординарная мысль, идея, вывод, приводится какой-либо цифрой материал, таблицу - обязательно сделайте ссылку на того автора у кого вы взяли данный материал.

5. Заключение содержит главные выводы, и итоги из текста основной части, в нем отмечается, как выполнены задачи и достигнуты ли цели, сформулированные во введении.

6. Приложение может включать графики, таблицы, расчеты.

7. Библиография (список литературы) здесь указывается реально использованная для написания реферата литература. Список составляется согласно правилам библиографического описания.

Этапы работы над рефератом.

Работу над рефератом можно условно подразделить на три этапа:

1. Подготовительный этап, включающий изучение предмета исследования;

2. Изложение результатов изучения в виде связного текста;

3. Устное сообщение по теме реферата.

1. Подготовительный этап работы.

Формулировка темы. Подготовительная работа над рефератом начинается с формулировки темы. Тема в концентрированном виде выражает содержание будущего текста, фиксируя как предмет исследования, так и его ожидаемый результат. Для того чтобы работа над рефератом была успешной, необходимо, чтобы тема заключала в себе проблему, скрытый вопрос (даже если наука уже давно дала ответ на этот вопрос, студент, только знакомящийся с соответствующей областью знаний, будет вынужден искать ответ заново, что даст толчок к развитию проблемного, исследовательского мышления).

Поиск источников. Грамотно сформулированная тема зафиксировала предмет изучения; задача обучающегося — найти информацию, относящуюся к данному предмету и разрешить поставленную проблему. Выполнение этой задачи начинается с поиска источников. На этом этапе необходимо вспомнить, как работать с энциклопедиями и энциклопедическими словарями.

Работа с источниками. Работу с источниками надо начинать с ознакомительного чтения, т. е. просмотреть текст, выделяя его структурные единицы. При ознакомительном чтении закладками отмечаются те страницы, которые требуют более внимательного изучения. В зависимости от результатов ознакомительного чтения выбирается дальнейший способ работы с источником. Если для разрешения поставленной задачи требуется изучение некоторых фрагментов текста, то используется метод выборочного чтения. Если в книге нет подробного оглавления, следует обратить внимание на предметные и именные указатели.

Избранные фрагменты или весь текст (если он целиком имеет отношение к теме) требуют вдумчивого, неторопливого чтения с «мысленной проработкой» материала. Такое чтение предполагает выделение: 1) главного в тексте; 2) основных аргументов; 3) выводов. Особое внимание следует обратить на то, вытекает тезис из аргументов или нет. Необходимо также проанализировать, какие из утверждений автора носят проблематичный, гипотетический характер и уловить скрытые вопросы.

Понятно, что умение таким образом работать с текстом приходит далеко не сразу. Наилучший способ научиться выделять главное в тексте, улавливать проблематичный характер утверждений, давать оценку авторской позиции — это сравнительное чтение, в ходе которого студент знакомится с различными мнениями по одному и тому же вопросу, сравнивает весомость и доказательность аргументов сторон и делает вывод о наибольшей убедительности той или иной позиции.

Создание конспектов для написания реферата.

Подготовительный этап работы завершается созданием конспектов, фиксирующих основные тезисы и аргументы. Здесь важно вспомнить, что конспекты пишутся на одной стороне листа, с полями и достаточным для исправления и ремарок межстрочным расстоянием (эти правила соблюдаются для удобства редактирования). Если в конспектах приводятся цитаты, то непременно должно быть дано указание на источник (автор, название, выходные данные, № страницы).

По завершении предварительного этапа можно переходить непосредственно к созданию текста реферата.

2. Создание текста.

Общие требования к тексту.

Текст реферата должен подчиняться определенным требованиям: он должен раскрывать тему, обладать связностью и цельностью.

Раскрытие темы предполагает, что в тексте реферата излагается относящийся к теме материал и предлагаются пути решения содержащейся в теме проблемы; связность текста предполагает смысловую соотносительность отдельных компонентов, а цельность - смысловую законченность текста.

С точки зрения связности все тексты делятся на тексты-констатации и тексты-рассуждения. Тексты-констатации содержат результаты ознакомления с предметом и

фиксируют устойчивые и несомненные суждения. В текстах-рассуждениях одни мысли извлекаются из других, некоторые ставятся под сомнение, дается им оценка, выдвигаются различные предположения.

План реферата.

Универсальный план реферата – введение, основной текст и заключение.

Требования к введению.

Во введении аргументируется актуальность исследования, - т. е. выявляется практическое и теоретическое значение данного исследования. Далее констатируется, что сделано в данной области предшественниками; перечисляются положения, которые должны быть обоснованы. Введение может также содержать обзор источников или экспериментальных данных, уточнение исходных понятий и терминов, сведения о методах исследования. Во введении обязательно формулируются цель и задачи реферата.

Объем введения - в среднем около 10% от общего объема реферата.

Основная часть реферата.

Основная часть реферата раскрывает содержание темы. Она наиболее значительна по объему, наиболее значима и ответственна. В ней обосновываются основные тезисы реферата, приводятся развернутые аргументы, предполагаются гипотезы, касающиеся существа обсуждаемого вопроса. Важно проследить, чтобы основная часть не имела форму монолога. Аргументируя собственную позицию, можно и должно анализировать, и оценивать позиции различных исследователей, с чем-то соглашаться, чему-то возражать, кого-то опровергать. Текст основной части делится на главы, параграфы, пункты. План основной части может быть составлен с использованием различных методов группировки материала: классификации (эмпирические исследования), типологии (теоретические исследования), периодизации (исторические исследования).

Заключение.

Заключение — последняя часть научного текста. В ней краткой и сжатой форме излагаются полученные результаты, представляющие собой ответ на главный вопрос исследования. Здесь же могут намечаться и дальнейшие перспективы развития темы. Небольшое по объему сообщение также не может обойтись без заключительной части - пусть это будут две-три фразы. Но в них должен подводиться итог проделанной работы.

Список использованной литературы.

Реферат любого уровня сложности обязательно сопровождается списком используемой литературы. Названия книг в списке располагают по алфавиту с указанием выходных данных использованных книг.

Требования, предъявляемыек оформлению реферата

Объемы рефератов – от 10-18 машинописных страниц. Работа выполняется на одной стороне листа стандартного формата. По обеим сторонам листа оставляются поля размером 35 мм. слева и 15 мм. справа, рекомендуется шрифт 12-14, интервал - 1,5. Все листы реферата должны быть пронумерованы. Каждый вопрос в тексте должен иметь заголовок в точном соответствии с наименованием в плане-оглавлении. При написании и оформлении реферата следует избегать типичных ошибок, например, таких:

– поверхностное изложение основных теоретических вопросов выбранной темы, когда автор не понимает, какие проблемы в тексте являются главными, а какие второстепенными,

– в некоторых случаях проблемы, рассматриваемые в разделах, не раскрывают основных аспектов выбранной для реферата темы,

– дословное переписывание книг, статей, заимствования рефератов из интернета и т. д.

При проверке реферата преподавателем оцениваются:

1. Знания и умения на уровне требований стандарта конкретной дисциплины: знание фактического материала, усвоение общих представлений, понятий, идей.

2. Характеристика реализации цели и задач исследования (новизна и актуальность

поставленных в реферате проблем, правильность формулирования цели, определения задач исследования, правильность выбора методов решения задач и реализации цели; соответствие выводов решаемым задачам, поставленной цели, убедительность выводов).

3. Степень обоснованности аргументов и обобщений (полнота, глубина, всесторонность раскрытия темы, логичность и последовательность изложения материала, корректность аргументации и системы доказательств, характер и достоверность примеров, иллюстративного материала, широта кругозора автора, наличие знаний интегрированного характера, способность к обобщению).

4. Качество и ценность полученных результатов (степень завершенности реферативного исследования, спорность или однозначность выводов).

5. Использование литературных источников.

6. Культура письменного изложения материала.

7. Культура оформления материалов работы.

ЛАБОРАТОРНЫЕ РАБОТЫ

Наименование раздела, темы дисциплины	Содержание лабораторных работ
Тема 1. Основы компьютерных преступлений	Классификация видов компьютерных преступлений: изучение основных категорий и типов компьютерных преступлений согласно законодательству РФ. Методы взлома компьютерных сетей и защита от них: практическое освоение методов выявления уязвимостей сетевых инфраструктур и способы защиты. Анализ вредоносного программного обеспечения: исследование структуры и функций вирусов, троянов, шпионских программ и других угроз информационной безопасности. Сбор цифровых доказательств компьютерного преступления: общие принципы и методы сбора электронных следов и цифровой информации.
Тема 2. Расследование компьютерных преступлений	Определение признаков состава преступления в сфере высоких технологий: определение квалификации уголовных деяний в области ИТ-правонарушений. Методология документирования и фиксации цифровых доказательств: порядок изъятия и закрепления доказательственных материалов при совершении киберпреступлений. Выявление следовых элементов при исследовании компьютерной техники подозреваемого лица: сбор цифровых следов, оставленных злоумышленником на устройстве жертвы
Тема 3. Противодействие компьютерным преступлениям, осуществляемым с использованием вредоносного программного обеспечения	Изучение классификации вредоносного ПО: анализ различных видов вредоносного программного обеспечения (вирусы, черви, трояны, руткиты). Методы обнаружения и идентификации вредоносного ПО: использование антивирусных сканеров и сигнатурных подходов для выявления зараженных объектов. Исследование механизмов распространения вредоносного ПО: изучение путей распространения вредоносных программ через электронную почту, веб-сайты, социальные сети и съемные носители.
Тема 4. Противодействие компьютерным	Работа с системами анализа трафика (IDS/IPS): применение межсетевых экранов и систем обнаружения вторжений для блокировки подозрительных пакетов данных. Подготовка отчетности по

Наименование раздела, темы дисциплины	Содержание лабораторных работ
преступлениям, реализуемым в ходе проведения компьютерных сетевых атак	инцидентам информационной безопасности: составление отчетов о выявленных случаях нарушения информационной безопасности предприятия. Моделируемые сценарии противодействия вредоносному ПО: отработка практических приемов реагирования на обнаружение вредоносных программ.
Тема 5. Противодействие компьютерным преступлениям путем реализации политики безопасности	Разработка политики безопасности в организации: основные этапы формирования и внедрения документационной политики информационной безопасности. Формулировка требований к защите данных и контроль исполнения: установление стандартов управления доступом и контроля над ресурсами предприятия. Регистрация и учет нарушений информационной безопасности: организация процедуры регистрации и учёта фактов несоблюдения установленных норм и правил.
Тема 6. Преступления в сфере компьютерной информации	Осуществление внутреннего аудита информационной безопасности: оценка соответствия текущих процессов стандартам и требованиям внутренней политики безопасности. Проведение тренингов сотрудников по вопросам информационной безопасности: осуществление регулярного информирования персонала относительно вопросов сохранения конфиденциальности и целостности данных. Организация и проведение проверок оборудования и каналов связи: проверка работоспособности защитного программного обеспечения и отсутствие неавторизованных подключений.
Тема 7. Компьютерные преступления, направленные на воздействие на критическую информационную инфраструктуру РФ	Критическая информационная инфраструктура (КИИ): определение и состав КИИ, роль КИИ в национальной безопасности, примеры объектов КИИ в России Типы угроз для КИИ: вредоносное ПО (вирусы, черви, трояны), атаки на отказ в обслуживании (DDoS), социальная инженерия и фишинг Методы и инструменты атак на КИИ: анализ уязвимостей систем, использование эксплойтов, примеры успешных атак на КИИ
Тема 8. Судебная практика по компьютерным преступлениям	Методы расследования компьютерных преступлений: сбор и анализ цифровых доказательств, использование экспертиз в судебном процессе, применение технологий для выявления и преследования преступников Роль прокурора и адвоката в делах о компьютерных преступлениях: обязанности и функции прокурора, защита прав обвиняемого и потерпевшего, стратегии защиты и обвинения Судебные процессы: этапы и особенности: подготовка к судебному разбирательству, проведение судебного заседания, принятие решений и вынесение приговоров
Тема 9. Предотвращение компьютерных преступлений	Политики безопасности информационных систем: разработка и внедрение политик безопасности, обучение сотрудников основам кибербезопасности, регулярные аудиты и тестирование систем. Социальная инженерия и методы защиты от нее: понятие социальной инженерии, примеры атак и способы защиты, обучение персонала

Критерии оценивания выполнения лабораторной работы:

Оценка «отлично» выставляется, если: работа выполнена в полном объеме с соблюдением необходимой последовательности действий; работа проведена в условиях, обеспечивающих получение правильных результатов и выводов; соблюдены правила техники безопасности; в ответе правильно и аккуратно выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполняет анализ ошибок.

Оценка «хорошо» выставляется, если: работа выполнена правильно с учетом 1-2 мелких погрешностей или 2-3 недочетов, исправленных самостоятельно по требованию преподавателя.

Оценка «удовлетворительно» выставляется, если: работа выполнена правильно не менее чем наполовину, допущены 1-2 погрешности или одна грубая ошибка.

Оценка «неудовлетворительно» выставляется, если: допущены две (и более) грубые ошибки в ходе работы, которые обучающийся не может исправить даже по требованию преподавателя или работа не выполнена полностью.

Типовые тесты

ТЕСТ № 1

1) К правовым методам, обеспечивающим информационную безопасность, относятся:

a) Разработка аппаратных средств обеспечения правовых данных
b) Разработка и установка во всех компьютерных правовых сетях журналов учета действий
c) Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:

a) Хищение жестких дисков, подключение к сети, инсайдерство
b) Перехват данных, хищение данных, изменение архитектуры системы
c) Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:

a) Персональная, корпоративная, государственная
b) Клиентская, серверная, сетевая
c) Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:

a) несанкционированного доступа, воздействия в сети
b) инсайдерства в организации
c) чрезвычайных ситуаций

5) Основные объекты информационной безопасности:

a) Компьютерные сети, базы данных
b) Информационные системы, психологическое состояние пользователей
c) Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:

a) Искажение, уменьшение объема, перекодировка информации

b) Техническое вмешательство, выведение из строя оборудования сети
c) Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:
a) Экономической эффективности системы безопасности
b) Многоплатформенной реализации системы
c) Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:
a) руководители, менеджеры, администраторы компаний
b) органы права, государства, бизнеса
c) сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:
a) Установление регламента, аудит системы, выявление рисков
b) Установка новых офисных приложений, смена хостинг-компании
c) Внедрение аутентификации, проверки контактных данных пользователей

10) Принципом информационной безопасности является принцип недопущения:
a) Неоправданных ограничений при работе в сети (системе)
b) Рисков безопасности сети, системы
c) Презумпции секретности

11) Принципом политики информационной безопасности является принцип:
a) Невозможности миновать защитные средства сети (системы)
b) Усиления основного звена сети, системы
c) Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:
a) Усиления защищенности самого незащищенного звена сети (системы)
b) Перехода в безопасное состояние работы сети, системы
c) Полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип:
a) Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
b) Одноуровневой защиты сети, системы
c) Совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:
a) Компьютерный сбой
b) Логические закладки («мины»)
c) Аварийное отключение питания

15) Когда получен спам по e-mail с приложенным файлом, следует:

a) Прочитать приложение, если оно не содержит ничего ценного –удалить
b) Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
c) Удалить письмо с приложением, не раскрывая (не читая) его

16) Принцип Кирхгофа:

a) Секретность ключа определена секретностью открытого сообщения
b) Секретность информации определена скоростью передачи данных
c) Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:

a) Электронно-цифровой преобразователь
b) Электронно-цифровая подпись
c) Электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:

a) Покупка нелицензионного ПО
b) Ошибки эксплуатации и неумышленного изменения режима работы системы
c) Сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:

a) Распределенный доступ клиент, отказ оборудования
b) Моральный износ сети, инсайдерство
c) Сбой (отказ) оборудования, нелегальное копирование данных

20) Наиболее распространены средства воздействия на сеть офиса:

a) Слабый трафик, информационный обман, вирусы в интернет
b) Вирусы в сети, логические мины (закладки), информационный перехват
c) Компьютерные сбои, изменение администрирования, топологии

21) Утечкой информации в системе называется ситуация, характеризуемая:

a) Потерей данных в системе
b) Изменением формы информации
c) Изменением содержания информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

a) Целостность
b) Доступность
c) Актуальность

23) Угроза информационной системе (компьютерной сети) – это:

a) Вероятное событие
b) Детерминированное (всегда определенное) событие
c) Событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам

сети, системы) называется:

a) Регламентированной
b) Правовой
c) Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:

a) Программные, технические, организационные, технологические
b) Серверные, клиентские, спутниковые, наземные
c) Личные, корпоративные, социальные, национальные

Критерии оценивания тестовых заданий для текущего контроля

Максимальное количество баллов за решение одного теста составляет 5 баллов, которые переводятся в академические оценки следующим образом:

- оценка «отлично» (5 баллов) выставляется при условии правильного ответа студента не менее чем на 85% контрольных заданий
- оценка «хорошо» (4 балла) выставляется при условии правильного ответа студента не менее чем на 70% контрольных заданий
- оценка «удовлетворительно» (3 балла) выставляется при условии правильного ответа студента не менее чем на 51% контрольных заданий
- оценка «неудовлетворительно» (1-2 балла) выставляется при условии правильного ответа студента менее чем на 50% контрольных заданий

ТЕСТ № 2

1. Основная масса угроз информационной безопасности приходится на:

а) Троянские программы
б) Шпионские программы
в) Черви

2. Какой вид идентификации и аутентификации получил наибольшее распространение:

а) системы PKI
б) постоянные пароли
в) одноразовые пароли

3. Под какие системы распространение вирусов происходит наиболее динамично:

а) Windows
б) Mac OS
в) Android

4. Заключительным этапом построения системы защиты является:

а) сопровождение
б) планирование
в) анализ уязвимых мест

5. Какие угрозы безопасности информации являются преднамеренными:

а) ошибки персонала
б) открытие электронного письма, содержащего вирус
в) не авторизованный доступ

6. Какой подход к обеспечению безопасности имеет место:

а) теоретический
б) комплексный
в) логический

7. Системой криптографической защиты информации является:
а) BFox Pro
б) CAudit Pro
в) Крипто Про

8. Какие вирусы активизируются в самом начале работы с операционной системой:
а) загрузочные вирусы
б) троянцы
в) черви

9. Stuxnet — это:
а) троянская программа
б) макровирус
в) промышленный вирус

10. Таргетированная атака — это:
а) атака на сетевое оборудование
б) атака на компьютерную систему крупного предприятия
в) атака на конкретный компьютер пользователя

11. Под информационной безопасностью понимается:
а) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре
б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия
в) нет верного ответа

12. Защита информации:
а) небольшая программа для выполнения определенной задачи
б) комплекс мероприятий, направленных на обеспечение информационной безопасности
в) процесс разработки структуры базы данных в соответствии с требованиями пользователей

13. Информационная безопасность зависит от:
а) компьютеров, поддерживающей инфраструктуры
б) пользователей
в) информации

14. Конфиденциальностью называется:
а) защита программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
б) описание процедур

в) защита от несанкционированного доступа к информации

15. Для чего создаются информационные системы:
а) получения определенных информационных услуг
б) обработки информации
в) оба варианта верны

16. Кто является основным ответственным за определение уровня классификации информации:
а) руководитель среднего звена
б) владелец
в) высшее руководство

17. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности:
а) хакеры
б) контрагенты
в) сотрудники

18. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству:
а) снизить уровень классификации этой информации
б) улучшить контроль за безопасностью этой информации
в) требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации

19. Что самое главное должно продумать руководство при классификации данных:
а) управление доступом, которое должно защищать данные
б) оценить уровень риска и отменить контрмеры
в) необходимый уровень доступности, целостности и конфиденциальности

20. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены:
а) владельцы данных
б) руководство
в) администраторы

Критерии оценивания тестовых заданий для текущего контроля

Максимальное количество баллов за решение одного теста составляет 5 баллов, которые переводятся в академические оценки следующим образом:

- оценка «отлично» (5 баллов) выставляется при условии правильного ответа студента не менее чем на 85% контрольных заданий
- оценка «хорошо» (4 балла) выставляется при условии правильного ответа студента не менее чем на 70% контрольных заданий
- оценка «удовлетворительно» (3 балла) выставляется при условии правильного ответа студента не менее чем на 51% контрольных заданий
- оценка «неудовлетворительно» (1-2 балла) выставляется при условии правильного ответа студента менее чем на 50% контрольных заданий

2.2 Оценочные материалы для проведения промежуточной

аттестации

1. С точки зрения криминалистических аспектов под компьютерными преступлениями следует понимать

a) предусмотренные уголовным законом общественно опасные действия, совершенные с использованием средств электронно-вычислительной (компьютерной) техники

b) предусмотренные уголовным законом общественно опасные действия, в которых машинная информация является объектом преступного посягательства

c) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ (т.е. машинной информации)

2. Все способы совершения компьютерных преступлений классифицируются в следующие общие группы:

a) изъятие средств компьютерной техники (СКТ); перехват информации; несанкционированный доступ к СКТ; манипуляция данными и управляющими командами; комплексные методы

b) перехват информации; несанкционированный доступ к СКТ; манипуляция данными и управляющими командами; комплексные методы

c) правовые; организационно-технические; программные

3. Основные группы мер предупреждения компьютерных преступлений:

a) правовые; организационно-технические; программные

b) организационно-технические; криминалистические

c) правовые; программные; криминалистические

4. Основная угроза безопасности информации – раскрытие конфиденциальной информации выражается в

a) несанкционированном доступе к БД, прослушивании каналов и т.п., т.е. это получение информации, являющейся достоянием некоторого лица другими лицами, в результате чего владельцам информации наносится существенный ущерб

b) внесении несанкционированных изменений в БД, в результате чего ее потребитель вынужден либо отказаться от нее, либо предпринять дополнительные усилия для выявления изменений и восстановления истинных сведений

c) получении одним из абонентов сведений, доступ к которым ему запрещен

d) непризнании получателем или отправителем информации фактов ее получения или отправки

5. Основная угроза безопасности информации – компрометация информации выражается в

a) внесении несанкционированных изменений в БД, в результате чего ее потребитель вынужден либо отказаться от нее, либо предпринять дополнительные усилия для выявления изменений и восстановления истинных сведений

b) несанкционированном доступе к БД, прослушивании каналов и т.п., т.е. это получение информации, являющейся достоянием некоторого лица другими лицами, в результате чего владельцам информации наносится существенный ущерб

c) получении одним из абонентов сведений, доступ к которым ему запрещен

d) непризнании получателем или отправителем информации фактов ее получения или отправки

6. В чем может быть выражен добровольный отказ пособника? (несколько

правильных ответов)
a) в отказе исполнителю до окончания им преступления в заранее обещанном содействии
b) в возмещении ущерба, причиненного преступлением;
c) в отказе от ранее обещанного содействия, заявленном исполнителю после окончания им преступления
d) в устранении результатов уже оказанной помощи

7. Установите соответствие между понятием и его утверждением
1. Преступление
2. Признаки преступления
3. Вина
4. Категории преступлений
a) Совершенное виновно общественно опасное деяние (действие или бездействие), запрещенное под угрозой уголовного наказания
b) Общественная опасность, виновность, противоправность, наказуемость
c) Психическое отношение лица к совершаемому им общественно опасному деянию и его общественно опасным последствиям
d) Виды преступлений, различающиеся по характеру и степени их общественной опасности

8. Основная угроза безопасности информации – несанкционированный обмен информацией между абонентами выражается в
a) получении одним из абонентов сведений, доступ к которым ему запрещен
b) внесении несанкционированных изменений в БД, в результате чего ее потребитель вынужден либо отказаться от нее, либо предпринять дополнительные усилия для выявления изменений и восстановления истинных сведений
c) несанкционированном доступе к БД, прослушивании каналов и т.п., т.е. это получение информации, являющейся достоянием некоторого лица другими лицами, в результате чего владельцам информации наносится существенный ущерб

9. Основная угроза безопасности – информации отказ от информации выражается в
a) непризнании получателем или отправителем информации фактов ее получения или отправки
b) получении одним из абонентов сведений, доступ к которым ему запрещен
c) внесении несанкционированных изменений в БД, в результате чего ее потребитель вынужден либо отказаться от нее, либо предпринять дополнительные усилия для выявления изменений и восстановления истинных сведений
d) несанкционированном доступе к БД, прослушивании каналов и т.п., т.е. это получение информации, являющейся достоянием некоторого лица другими лицами, в результате чего владельцам информации наносится существенный ущерб

10. Основная угроза безопасности информации – отказ в обслуживании выражается в
a) неправильной работе самой ИС, является весьма существенной и распространенной угрозой
b) непризнании получателем или отправителем информации фактов ее получения или отправки
c) получении одним из абонентов сведений, доступ к которым ему запрещен
d) внесении несанкционированных изменений в БД, в результате чего ее потребитель вынужден либо отказаться от нее, либо предпринять дополнительные усилия для

выявления изменений и восстановления истинных сведений

11. Препятствие – это метод защиты информации путем
a) физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.п.)
- побуждения пользователей ИС не разрушать установленные порядки за счет соблюдения сложившихся моральных и этических норм, как регламентированных, так и неписаных
b) регулирования использования всех ресурсов ИС и выполнения таких функций как идентификация объекта, опознание объекта по предъявленному им идентификатору, проверку полномочий; разрешение и создание условий работы в пределах установленного регламента, регистрацию обращений к защищаемым ресурсам, регулирование при попытках несанкционированных действий
c) вынуждения пользователей и персонала ИС соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности

12. Управление доступом – это метод защиты информации путем
a) регулирования использования всех ресурсов ИС и выполнения таких функций как идентификация объекта, опознание объекта по предъявленному им идентификатору, проверку полномочий; разрешение и создание условий работы в пределах установленного регламента, регистрацию обращений к защищаемым ресурсам, регулирование при попытках несанкционированных действий
b) побуждения пользователей ИС не разрушать установленные порядки за счет соблюдения сложившихся моральных и этических норм, как регламентированных, так и неписаных
c) вынуждения пользователей и персонала ИС соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности

13. Маскировка – это метод защиты информации путем
a) ее криптографического закрытия
b) регулирования использования всех ресурсов ИС и выполнения таких функций как идентификация объекта, опознание объекта по предъявленному им идентификатору, проверку полномочий; разрешение и создание условий работы в пределах установленного регламента, регистрацию обращений к защищаемым ресурсам, регулирование при попытках несанкционированных действий
c) вынуждения пользователей и персонала ИС соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности
d) физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.п.)

14. Регламентация – это метод защиты информации путем
a) создания такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму
b) побуждения пользователей ИС не разрушать установленные порядки за счет соблюдения сложившихся моральных и этических норм, как регламентированных, так и неписаных
c) регулирования использования всех ресурсов ИС и выполнения таких функций как идентификация объекта, опознание объекта по предъявленному им идентификатору,

проверку полномочий; разрешение и создание условий работы в пределах установленного регламента, регистрацию обращений к защищаемым ресурсам, регулирование при попытках несанкционированных действий

15. Принуждение – это метод защиты информации путем

a) вынуждения пользователей и персонала ИС соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности

b) побуждения пользователей ИС не разрушать установленные порядки за счет соблюдения сложившихся моральных и этических норм, как регламентированных, так и неписаных

c) регулирования использования всех ресурсов ИС и выполнения таких функций как идентификация объекта, опознание объекта по предъявленному им идентификатору, проверку полномочий;

d) разрешение и создание условий работы в пределах установленного регламента, регистрацию обращений к защищаемым ресурсам, регулирование при попытках несанкционированных действий

16. Расположите в хронологическом порядке следующие информационные войны
a) «Бархатные» революции в странах Восточной Европы
b) Августовский путч в СССР
c) Агрессия в Югославии
d) «Революция роз» в Грузии
e) «Оранжевая революция» в Украине
f) Гуманитарная катастрофа в Южной Осетии

17. Установите соответствия между определением и его утверждением
1. история оружия в гуманитарной сфере
2. история оружия в технической сфере
a) это история СМИ и технологий скрытного управления человеком (гипноз, реклама, специальные учения, НЛП-программирование и т.п.)
b) это история программных средств скрытого информационного воздействия (вирусы, закладки) и информационных технологий их применения

18. В главе 28 "Преступления в сфере компьютерной информации" УК РФ определяются следующие общественно-опасные деяния в отношении средств компьютерной техники:

a) неправомерный доступ к охраняемой законом компьютерной информации; создание вредоносных программ для ЭВМ; нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

b) финансовое мошенничество; кража конфиденциальной информации; мошенничество, касающееся средств связи; несанкционированный доступ; диверсия; проникновение в систему

c) несанкционированный доступ к информации; применение не сертифицированных программ и баз данных; создание вирусных программ

19. Основными мотивами при совершении компьютерных преступлений являются

a) корыстные, политические, исследовательский интерес, хулиганство и озорство, месть

b) корыстные, политические

c) хулиганство и озорство

20. Основными опасными субъектами неправомерного доступа к компьютерной информации являются(несколько правильных ответов)

a) граждане и юридические лица
b) хакеры-исследователи, хакеры взломщики, хакеры-вандалы
c) крэкеры, компьютерные пираты, кибертеррористы

21. Хакеры-исследователи – люди

a) образованные и талантливые, основным занятием которых является анализ разнообразного программного обеспечения на уязвимости, которыми может воспользоваться потенциальный взломщик или которые могут улучшить работу компьютерной системы, сети, увеличивая ее эффективность
b) осуществляющие по различным целям взлом, проникновение, при котором никакая информация не была уничтожена на каких-либо носителях, система продолжала работать без снижения своей эффективности, после проникновения хакер сообщил соответствующим лицам, ответственным за безопасность данной системы о проникновении, способе проникновения и подробно описал процедуру вторжения
c) специализирующиеся на изучении особенностей кредитных карт и банкоматов

22. Хакеры-взломщики – люди

a) осуществляющие по различным целям взлом, проникновение, при котором никакая информация не была уничтожена на каких-либо носителях, система продолжала работать без снижения своей эффективности, после проникновения хакер сообщил соответствующим лицам, ответственным за безопасность данной системы о проникновении, способе проникновения и подробно описал процедуру вторжения
b) по каким-то причинам планирующие и осуществляющие вторжение в компьютерные системы с сознательной целью причинения ущерба этим системам
c) которые целенаправленно занимаются коммерческим взломом компьютерных систем и сетей в корыстных целях

23. Хакеры-вандалы – люди

a) по каким-то причинам планирующие и осуществляющие вторжение в компьютерные системы с сознательной целью причинения ущерба этим системам
b) которые целенаправленно занимаются коммерческим взломом компьютерных систем и сетей в корыстных целях
c) которые специализируются на взломе программного обеспечения для последующей продажи

24. Компьютерные пираты – люди

a) чаще всего группы, которые специализируются на взломе программного обеспечения для последующей продажи
b) целенаправленно занимаются коммерческим взломом компьютерных систем и сетей в корыстных целях
c) по каким-то причинам планирующие и осуществляющие вторжение в компьютерные системы с сознательной целью причинения ущерба этим системам

25. Кибертеррористы – люди

a) которые целенаправленно стараются причинить вред государству или какой-то группе людей, по идеологическим соображениям, по возможности, максимизируя причиненный ущерб
b) по каким-то причинам планирующие и осуществляющие вторжение в компьютерные системы с сознательной целью причинения ущерба этим системам

c) чаще всего группы, которые специализируются на взломе программного обеспечения для последующей продажи

26. Вирмейкеры – люди

a) занимаются написанием компьютерных вирусов

b) целенаправленно стараются причинить вред государству или какой-то группе людей, по идеологическим соображениям, по возможности, максимизируя причиненный ущерб

c) чаще всего группы, которые специализируются на взломе программного обеспечения для последующей продажи

27. Установите соответствия между определением и его утверждением

1. Вирмейкеры – люди
2. Кибертеррористы – люди
3.Компьютерные пираты – люди

А) занимаются написанием компьютерных вирусов

Б) которые целенаправленно стараются причинить вред государству или какой-то группе людей, по идеологическим соображениям, по возможности, максимизируя причиненный ущерб

В) чаще всего группы, которые специализируются на взломе программного обеспечения для последующей продажи

28. С точки зрения уголовно-правовой охраны под компьютерными преступлениями следует понимать

a) предусмотренные уголовным законом общественно опасные действия, в которых машинная информация является объектом преступного посягательства
b) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ (т.е. машинной информации)
c) предусмотренные уголовным законом общественно опасные действия, совершенные с использованием средств электронно-вычислительной (компьютерной) техники

29. С точки зрения криминалистических аспектов под компьютерными преступлениямиследует понимать

a) предусмотренные уголовным законом общественно опасные действия, совершенные с использованием средств электронно-вычислительной (компьютерной) техники

b) предусмотренные уголовным законом общественно опасные действия, в которых машинная информация является объектом преступного посягательства

c) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ (т.е. машинной информации)

30. Юридическая ответственность за информационные правонарушения - это

a) применение к виновному лицу, совершившему правонарушение, мер воздействия, предусмотренных санкцией нарушенной нормы информационного права в определенном регламентированном порядке

b) применение к виновному лицу, совершившему правонарушение, установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) и правил защиты информации, мер воздействия, предусмотренных санкцией нарушенной нормы информационного права в

определенном регламентированном порядке

c) ответственность работников, по вине которых предприятие, учреждение, организация понесли расходы по возмещению вреда

31. Состав информационного правонарушения включает в себя следующие элементы (признаки)

a) объект, объективную сторону, субъект и субъективную сторону
b) объект, субъект, поведение, право, обязанность, ответственность
c) общественные отношения, физические и юридические лица, ответственность

32. К специальным признакам информационного правонарушения относятся (несколько вариантов)

a) информационная сфера, информационная среда их совершения
b) использование информационных средств и технологий
c) противоправность, общественная опасность, деликтоспособность и виновность
d) информационная сфера, противоправность, общественная опасность, деликтоспособность
e) деликтоспособность и виновность

33. Информационное преступление это _

34. Дисциплинарная ответственность предусматривает следующие меры Наказания_____

35. Меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе

a) Информационная безопасность
b) Защитные технологии
c) Заземление
d) Конфиденциальность

Критерии оценки для проведения зачета по дисциплине (тестирование)

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 наименование кафедры
от ___ _____ 20_ г., протокол № ___

одобрено Научно-методическим советом _____ от ___ _____ 20__ г., протокол №____