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

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

ОРГАНИЗАЦИЯ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Специальность: 10.05.01 Компьютерная безопасность
Специализация: «Разработка защищенного программного обеспечения»
Формы обучения: очная
Объем дисциплины:
в зачетных единицах: 4 з.е.
в академических часах: 144 ак.ч.

Форма промежуточной аттестации: экзамен

2025

Оценочные материалы по дисциплине Организация и правовое обеспечение информационной безопасности

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 Организация и правовое обеспечение информационной безопасности 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 Организация и правовое обеспечение информационной безопасности.

1.Паспорт оценочных материалов по дисциплине «Организация и правовое обеспечение информационной безопасности»

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения	Контролируемые разделы, темы дисциплины	Наименование оценочного средства	
				Текущий контроль	Промежуточная аттестация
1	2	3	4	5	6
ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации	ОПК-9.2 Демонстрирует умение решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития сетей и систем передачи информации	Знать основные принципы работы с данными, современные инструменты анализа данных на базовом уровне, в том числе навыки программирования, алгоритмизации и математические методы при решении задач анализа данных Уметь выбирать и применять средства защиты информационных систем, компьютерных сетей, баз данных, операционных систем, технических каналов утечки информации. Владеть нормативно-правовой информацией, регламентирующей вопросы защиты информации, и применение её в профессиональной деятельности	Тема 1. Характеристика правоотношений в сфере защиты информации. Тема 2. Структура системы организационно-правового обеспечения информационной безопасности. Тема 3. Нормативно-правовая база обеспечения защиты информации в России. Тема 4. Угрозы информационной безопасности.	Опрос (Тема 1-5) Доклад /Презентация (Тема 1-5) Тест (Тема 1-5)	Тест (П 1-7 тестового задания)
ОПК-10 Способен анализировать	ОПК-10.3 Демонстрирует	Знать: основные типы криптографических протоколов и принципы их построения с	Тема 1. Характеристика	Опрос (Тема 1-5)	Тест (П 8-14 тестового задания)

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения	Контролируемые разделы, темы дисциплины	Наименование оценочного средства	
				Текущий контроль	Промежуточная аттестация
1	2	3	4	5	6
тенденции развития методов и средств криптографическо й защиты информации, использовать средства криптографическо й защиты информации при решении задач профессиональной деятельности	умения разработки криптографически х протоколов и исследования их стойкости к различным атакам в составе средств защиты компьютерных систем	использованием шифрсистем, основные стандарты, протоколы и интерфейсы, необходимые при сертификации средств защиты информации Уметь: проводить анализ криптографических протоколов, применять криптографические средства и системы информационной безопасности Владеть: математическими методами при использовании криптографических протоколов, государственными стандартами	правоотношений в сфере защиты информации. Тема 2. Структура системы организационно-правового обеспечения информационной безопасности. Тема 3. Нормативно-правовая база обеспечения защиты информации в России. Тема 4. Угрозы информационной безопасности. Угрозы информационной безопасности.	Доклад /Презентация (Тема 1-5) Тест (Тема 1-5	

2. Оценочные материалы по дисциплине Организация и правовое обеспечение информационной безопасности

2.1 Оценочные материалы для проведения текущего контроля успеваемости

Тема 1. Характеристика правоотношений в сфере защиты информации.

Вопросы для опроса:

1. Информация и окружающий мир.
2. Свойства информации. Влияние информации на общество.
3. Информация и право.
4. Правовое определение понятия "информация".
5. Документирование информации.
6. Понятие информационных ресурсов.
7. Виды информации по категориям доступа.
8. Общедоступная информация.
9. Информация ограниченного доступа.
10. Информационные технологии.
11. Правовое закрепление необходимости принятия мер по защите информации.
12. Составление правовых понятий информационной безопасности и защиты информации.
13. Объекты и субъекты сферы защиты информации. Цели защиты информации.

Цель опроса – закрепить полученные знания и развить профессиональные навыки и умения, актуальные для будущих специальстов.

Критерии оценки:

«отлично» - ставится обучающемуся, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений;

«хорошо» - ставится обучающемуся, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;

«удовлетворительно» - ставится обучающемуся, показавшему фрагментарный, разрозненный характер знаний и может применять полученные знания по образцу в стандартной ситуации;

«неудовлетворительно» - ставится студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении практических задач

Тематика докладов/презентаций:

1. Модели сетевой безопасности и безопасности информационной системы.
2. Стандарты информационной безопасности (их роль и значение).
3. Международные и отечественные стандарты информационной безопасности.
4. Соблюдение основных требований к информационной безопасности.

Критерии оценки докладов:

– оценка *«отлично»* выставляется студенту, если выполнены все требования к написанию и защите доклада: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.

– оценка *«хорошо»,* если основные требования к докладу и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём доклада; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.

– оценка *«удовлетворительно»,* если имеются существенные отступления от требований. В частности, тема освещена лишь частично; допущены фактические ошибки в содержании доклада или при ответе на дополнительные вопросы; во время защиты отсутствует вывод.

– оценка *«неудовлетворительно»* тема доклада не раскрыта, обнаруживается существенное непонимание проблемы.

Тесты по теме:

1. Как называется информация, которую следует защищать (по нормативам, правилам сети, системы)?
а) Регламентированной
б) Правовой
в) Защищаемой+

2. Разновидностями угроз безопасности (сети, системы) являются:
а) Программные, технические, организационные, технологические+
б) Серверные, клиентские, спутниковые, наземные
в) Личные, корпоративные, социальные, национальные

3. Относятся к правовым методам, обеспечивающим информационную безопасность:
а) Разработка аппаратных средств обеспечения правовых данных
б) Разработка и установка во всех компьютерных правовых сетях журналов учета действий
в) Разработка и конкретизация правовых нормативных актов обеспечения безопасности+

4. Основные источники угроз информационной безопасности:
а) Хищение жестких дисков, подключение к сети, инсайдерство
б) Перехват данных, хищение данных, изменение архитектуры системы+
в) Хищение данных, подкуп системных администраторов, нарушение регламента работы

5. Выберите виды информационной безопасности:
а) Персональная, корпоративная, государственная+
б) Клиентская, серверная, сетевая
в) Локальная, глобальная, смешанная

6. Цели информационной безопасности – своевременное обнаружение, предупреждение:
а) несанкционированного доступа, воздействия в сети+
б) инсайдерства в организации
в) чрезвычайных ситуаций

Критерии оценки тестов:
85% – 100% правильных ответов – «отлично»;
75% – 84% правильных ответов – «хорошо»;
50% – 75% правильных ответов – «удовлетворительно»;
менее 50 % правильных ответов – «неудовлетворительно».

Тема 2. Структура системы организационно-правового обеспечения информационной безопасности.

Вопросы для опроса:

1. Определение понятия «Комплексная система защиты информации» и элементы этой системы.
2. Понятие "Организационная защита информации".
3. Сущность организационных методов защиты информации.
4. Соотношение организационных методов защиты информации с правовыми и техническими.
5. Организационные методы как реализация полномочий и их распределение между уровнями управления организацией.
6. Особенности нормативно- правового регулирования современных отношений в сфере защиты информации.

Цель опроса – закрепить полученные знания и развить профессиональные навыки и умения, актуальные для будущих специальстов.

Критерии оценки:

«отлично» - ставится обучающемуся, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений;

«хорошо» - ставится обучающемуся, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;

«удовлетворительно» - ставится обучающемуся, показавшему фрагментарный, разрозненный характер знаний и может применять полученные знания по образцу в стандартной ситуации;

«неудовлетворительно» - ставится студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении практических задач

Тематика докладов/презентаций:

1. Криптостойкость.
2. Симметричные криптосистемы шифрования.
3. Асимметричные системы шифрования.
4. Алгоритм RSA.
5. Хэш-функции и аутентификация сообщений MD5, ГОСТ 3411.
6. Стандарты ЭЦП: DSS, ГОСТ 3410.
7. Инфраструктура управления открытыми ключами PKI.

Критерии оценки докладов:

– оценка *«отлично»* выставляется студенту, если выполнены все требования к написанию и защите доклада: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.

– оценка *«хорошо»,* если основные требования к докладу и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём доклада; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.

– оценка *«удовлетворительно»,* если имеются существенные отступления от требований. В частности, тема освещена лишь частично; допущены фактические ошибки в содержании доклада или при ответе на дополнительные вопросы; во время защиты отсутствует вывод.

– оценка *«неудовлетворительно»* тема доклада не раскрыта, обнаруживается существенное непонимание проблемы.

Тесты по теме:

1. Основными объектами информационной безопасности являются:
а) Компьютерные сети, базы данных+
б) Информационные системы, психологическое состояние пользователей
в) Бизнес-ориентированные, коммерческие системы

2. Утечка информации в системе:
а) это ситуация, которая характеризуется потерей данных в системе+
б) это ситуация, которая характеризуется изменением формы информации
в) это ситуация, которая характеризуется изменением содержания информации

3. Выберите наиболее важный момент при реализации защитных мер политики безопасности :
а) Аудит, анализ затрат на проведение защитных мер
б) Аудит, анализ безопасности
в) Аудит, анализ уязвимостей, риск-ситуаций+

4. Определите, какой подход к обеспечению безопасности имеет место:
а) теоретический
б) комплексный +
в) логический

5. Система криптографической защиты информации:
а) BFox Pro
б) CAudit Pro
в) Крипто Про +

6. Вирусы, которые активизируются в самом начале работы с операционной системой:
а) загрузочные вирусы +
б) троянцы
в) черви

Критерии оценки тестов:
85% – 100% правильных ответов – «отлично»;
75% – 84% правильных ответов – «хорошо»;
50% – 75% правильных ответов – «удовлетворительно»;
менее 50 % правильных ответов – «неудовлетворительно».

Тема 3. Нормативно-правовая база обеспечения защиты информации в России.

Вопросы для опроса:

1. Особенности нормативно-правового регулирования современных отношений в сфере защиты информации.
2. Конституционное законодательство о защите информации.
3. Доктрина
4. информационной безопасности Российской Федерации.
5. Обзор законодательных актов общего характера, содержащих положения о защите информации.
6. Специальное законодательство по защите информации.
7. Особая роль законов «Об информации, информационных технологиях и защите информации», «О коммерческой тайне», «О государственной тайне», "О персональных данных", "Об электронной подписи", "Об оперативно-розыскной деятельности", "О техническом регулировании», "О безопасности критической информационной инфраструктуры Российской Федерации".
8. Законы субъектов РФ, регламентирующие вопросы защиты информации.
9. Подзаконные правовые акты, регулирующие процессы защиты информации.
10. Роль подзаконных нормативных документов ФСТЭК РФ и ФСБ РФ.
11. Основные документы ФСТЭК России определяющие требования по защите информации.
12. Нормативно-правовые акты, устанавливающие юридическую ответственность за правонарушения в сфере защиты информации.

Цель опроса – закрепить полученные знания и развить профессиональные навыки и умения, актуальные для будущих специальстов.

Критерии оценки:

«отлично» - ставится обучающемуся, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений;

«хорошо» - ставится обучающемуся, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;

«удовлетворительно» - ставится обучающемуся, показавшему фрагментарный, разрозненный характер знаний и может применять полученные знания по образцу в стандартной ситуации;

«неудовлетворительно» - ставится студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины

и не умеет использовать полученные знания при решении практических задач

Тематика докладов/презентаций:

1. Аутентификация, авторизация и администрирование действий пользователей.
2. Биометрическая аутентификация пользователей.
3. Управление идентификацией и доступом.
4. Обеспечение безопасности и целостности данных в информационных системах.

Критерии оценки докладов:

– оценка *«отлично»* выставляется студенту, если выполнены все требования к написанию и защите доклада: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.

– оценка *«хорошо»,* если основные требования к докладу и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём доклада; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.

– оценка *«удовлетворительно»,* если имеются существенные отступления от требований. В частности, тема освещена лишь частично; допущены фактические ошибки в содержании доклада или при ответе на дополнительные вопросы; во время защиты отсутствует вывод.

– оценка *«неудовлетворительно»* тема доклада не раскрыта, обнаруживается существенное непонимание проблемы.

Тесты по теме:

1. Кто в итоге несет ответственность за защищенность данных в компьютерной сети?
а) Владелец сети+
б) Администратор сети
в) Пользователь сети

2. Политика безопасности в системе (сети) – это комплекс:
а) Руководств, требований обеспечения необходимого уровня безопасности+
б) Инструкций, алгоритмов поведения пользователя в сети
в) Нормы информационного права, соблюдаемые в сети

3. Наиболее важным при реализации защитных мер политики безопасности является следующее:
а) Аудит, анализ затрат на проведение защитных мер
б) Аудит, анализ безопасности
в) Аудит, анализ уязвимостей, риск-ситуаций+

4. Свойство информации, наиболее актуальное при обеспечении информационной безопасности:
а) Целостность+
б) Доступность
в) Актуальность

5. 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

6. Выберите, 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 +

Критерии оценки тестов:
85% – 100% правильных ответов – «отлично»;
75% – 84% правильных ответов – «хорошо»;
50% – 75% правильных ответов – «удовлетворительно»;
менее 50 % правильных ответов – «неудовлетворительно».

Тема 4. Угрозы информационной безопасности.

Вопросы для опроса:

1. Основные понятия.
2. Классификация угроз.
3. Источники и каналы утечки информации.

Цель опроса – закрепить полученные знания и развить профессиональные навыки и умения, актуальные для будущих специальстов.

Критерии оценки:

«отлично» - ставится обучающемуся, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений;

«хорошо» - ставится обучающемуся, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;

«удовлетворительно» - ставится обучающемуся, показавшему фрагментарный, разрозненный характер знаний и может применять полученные знания по образцу в стандартной ситуации;

«неудовлетворительно» - ставится студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении практических задач

Тематика докладов/презентаций:

1. Архитектура подсистемы защиты операционной системы.
2. Обеспечение безопасности ОС UNIX и Windows.
3. Защита беспроводных сетей.
4. Безопасность в открытых сетях.
5. Инфраструктура цифровых сертификатов.
6. Функции межсетевых экранов.
7. Схемы сетевой защиты на базе межсетевых экранов.

Критерии оценки докладов:

– оценка *«отлично»* выставляется студенту, если выполнены все требования к написанию и защите доклада: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.

– оценка *«хорошо»,* если основные требования к докладу и его

защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём доклада; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.

– оценка *«удовлетворительно»,* если имеются существенные отступления от требований. В частности, тема освещена лишь частично; допущены фактические ошибки в содержании доклада или при ответе на дополнительные вопросы; во время защиты отсутствует вывод.

– оценка *«неудовлетворительно»* тема доклада не раскрыта, обнаруживается существенное непонимание проблемы.

Тесты по теме:

1. Когда получен спам по e-mail с приложенным файлом, следует:
а) Прочитать приложение, если оно не содержит ничего ценного – удалить
б) Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
в) Удалить письмо с приложением, не раскрывая (не читая) его+

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

3. Конфиденциальность:
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 +

4. Определите, для чего создаются информационные системы:
а) получения определенных информационных услуг +
б) обработки информации
в) оба варианта верны

5. Наиболее распространены средства воздействия на сеть офиса:
а) Слабый трафик, информационный обман, вирусы в интернет
б) Вирусы в сети, логические мины (закладки), информационный перехват+
в) Компьютерные сбои, изменение администрирования, топологии

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

Критерии оценки тестов:
85% – 100% правильных ответов – «отлично»;
75% – 84% правильных ответов – «хорошо»;
50% – 75% правильных ответов – «удовлетворительно»;
менее 50 % правильных ответов – «неудовлетворительно».

Тема 5. Силы и средства организационной защиты информации.

Вопросы для опроса:

1. Служба информационной безопасности предприятия.
2. Состав, задачи, основные направления деятельности службы информационной безопасности предприятия.
3. Основные направления деятельности по взаимодействию с правоохранительными органами и службами обеспечения информационной безопасности.
4. Политика информационной безопасности предприятия.

Цель опроса – закрепить полученные знания и развить профессиональные навыки и умения, актуальные для будущих специальстов.

Критерии оценки:

«отлично» - ставится обучающемуся, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений;

«хорошо» - ставится обучающемуся, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;

«удовлетворительно» - ставится обучающемуся, показавшему фрагментарный, разрозненный характер знаний и может применять полученные знания по образцу в стандартной ситуации;

«неудовлетворительно» - ставится студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении практических задач

Тематика докладов/презентаций:

5. Особенности удаленного доступа.
6. Протокол Kerberos.
7. Система IPS.
8. Классификация вредоносных программ.
9. Защита ИС от вирусов и вредоносных программ.

Критерии оценки докладов:

– оценка *«отлично»* выставляется студенту, если выполнены все требования к написанию и защите доклада: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на

дополнительные вопросы.

– оценка *«хорошо»,* если основные требования к докладу и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём доклада; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.

– оценка *«удовлетворительно»,* если имеются существенные отступления от требований. В частности, тема освещена лишь частично; допущены фактические ошибки в содержании доклада или при ответе на дополнительные вопросы; во время защиты отсутствует вывод.

– оценка *«неудовлетворительно»* тема доклада не раскрыта, обнаруживается существенное непонимание проблемы.

Тесты по теме:

1. Отметьте категорию, которая является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности:
а) хакеры
б) контрагенты
в) сотрудники +

2. Что такое угроза информационной системе (компьютерной сети)?
а) Вероятное событие+
б) Детерминированное (всегда определенное) событие
в) Событие, происходящее периодически

3. Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
а) Регламентированной
б) Правовой
в) Защищаемой+

4. Разновидностями угроз безопасности (сети, системы) являются:
а) Программные, технические, организационные, технологические+
б) Серверные, клиентские, спутниковые, наземные
в) Личные, корпоративные, социальные, национальные

5. Какие угрозы безопасности информации являются преднамеренными?
а) ошибки персонала
б) открытие электронного письма, содержащего вирус
в) не авторизованный доступ +

6. Что такое stuxnet?

а) троянская программа

б) макровирус

в) промышленный вирус +

Критерии оценки тестов:

85% – 100% правильных ответов – «отлично»;

75% – 84% правильных ответов – «хорошо»;

50% – 75% правильных ответов – «удовлетворительно»;

менее 50 % правильных ответов – «неудовлетворительно».

Доклад – публичное сообщение на определенную тему, способствующее формированию навыков исследовательской работы, расширяющее познавательный интерес.

Работа над докладом состоит из следующих этапов:

- составление плана работы;
- систематизации полученных сведений;
- составление выводов и обобщений.

Доклад предоставляется в письменной форме.

Письменный доклад – это запись устного сообщения по какой-либо теме объёмом от пяти до пятнадцати страниц. В таком докладе не обязательно:

- выделять структурные элементы работы в виде плана;
- выделять заголовки внутри текста;
- ссылаться на использованную литературу по ходу текста.

Но обязательно следует приводить список всех используемых источников в конце работы. При подготовке доклада целесообразно соблюдать следующий порядок работы:

1. Подобрать литературу по изучаемой теме, познакомиться с её содержанием.
2. Пользуясь закладками, отметить наиболее существенные места или сделать выписки.
3. Составить план доклада.
4. Используя рекомендации по составлению тематического конспекта и составленный план, написать доклад, в заключение которого обязательно выразить своё отношение к излагаемой теме и её содержанию.
5. Прочитать текст и редактировать его.
6. Оформить в соответствии с требованиями к оформлению докладов

Тест – это система формализованных заданий, по результатам выполнения которых можно измерить уровень знаний, умений и навыков обучающегося.

2.2 Оценочные материалы для проведения промежуточной аттестации

Вопросы к экзамену:

1. Основные понятия защиты информации: атаки, уязвимости, политика безопасности, механизмы и сервисы безопасности.
2. Классификация угроз ИБ.
3. Модели сетевой безопасности и безопасности информационной системы.
4. Анализ угроз информационной безопасности.
5. Стандарты информационной безопасности (их роль и значение).
6. Международные и отечественные стандарты информационной безопасности.
7. Уровни информационной защиты (безопасности).
8. Основные понятия криптографической защиты информации.
9. Криптостойкость. Традиционное шифрование: классические методы.
10. Симметричные криптосистемы шифрования.
11. Блочные и поточные алгоритмы симметричного шифрования.
12. Стандарты и алгоритмы: американский DES, отечественный ГОСТ 28147, режимы их выполнения.
13. Асимметричные системы шифрования. RSA.
14. Криптография с использованием эллиптических кривых.
15. Хэш-функции и аутентификация сообщений MD5, ГОСТ 3411.
16. Электронная цифровая подпись (ЭЦП). Стандарты ЭЦП: DSS, ГОСТ 3410.
17. Управление криптоключами.
18. Инфраструктура управления открытыми ключами PKI.
19. Аутентификация, авторизация и администрирование действий пользователей.
20. Пароли. Строгая аутентификация.
21. Биометрическая аутентификация пользователей.
22. Управление доступом по схеме однократного входа.
23. Управление идентификацией и доступом.
24. Защита электронного документооборота.
25. Проблемы обеспечения безопасности ОС.
26. Архитектура подсистемы защиты операционной системы.
27. Обеспечение безопасности ОС UNIX и Windows.
28. Защита на канальном уровне – протоколы PPTP/
29. Защита на сетевом уровне – протокол IPSec.
30. Защита на сеансом уровне – протоколы SSL/TLS.
31. Защита беспроводных сетей.
32. Безопасность в открытых сетях.
33. Инфраструктура цифровых сертификатов.
34. Межсетевое экранирование. Функции межсетевых экранов.

35. Особенности функционирования межсетевых экранов на различных уровнях модели OSI.
36. Схемы сетевой защиты на базе межсетевых экранов.
37. Особенности удаленного доступа.
38. Организация защищенного удаленного доступа.
39. Протокол Kerberos.
40. Обнаружение и предотвращение вторжений. Система IPS.
41. Классификация вредоносных программ.
42. Основы работы антивирусных программ.
43. Защита ИС от вирусов и вредоносных программ.

Тестовые задания для проведения промежуточной аттестации

П 1. Включение в число основных аспектов безопасности подотчетности...
правильно, потому что без подотчетности не может быть безопасности
неправильно, потому что подотчетность - не цель, а средство достижения безопасности+
не имеет значения, потому что далека от реальной безопасности

П 2. На законодательном уровне информационной безопасности особенно важны:
направляющие и координирующие меры+
ограничительные меры
меры по обеспечению информационной независимости

П 3. Принцип усиления самого слабого звена можно переформулировать как:
принцип равнопрочности обороны+
принцип удаления слабого звена
принцип выявления главного звена, ухватившись за которое, можно вытянуть всю цепь

П 4. Нужно ли включать в число ресурсов по информационной безопасности серверы с информацией органов лицензирования и сертификации по данной тематике:
да, поскольку наличие лицензий и сертификатов при прочих равных условиях является важным достоинством+
нет, поскольку реально используемые продукты все равно не могут быть сертифицированы
не имеет значения, поскольку если информация о лицензиях или сертификатах понадобится, ее легко найти

П 5. Информационная безопасность - это дисциплина:
комплексная+
техническая
программистская

П 6. Сервисы безопасности подразделяются на:
глобализующие, расширяющие зону поиска нарушителя
локализующие, сужающие зону воздействия нарушений+
буферизующие, сглаживающие злоумышленную активность

П 7. Политика безопасности:
фиксирует правила разграничения доступа-
отражает подход организации к защите своих информационных активов+
описывает способы защиты руководства организации

П 8. Протоколирование само по себе не может обеспечить неотказуемость, потому что:
регистрационная информация может быть рассредоточена по разным сервисам и разным компонентам распределенной ИС-
целостность регистрационной информации может быть нарушена+
должна соблюдаться конфиденциальность регистрационной информации, а проверка неотказуемости нарушит конфиденциальность

П 9. В число этапов управления рисками входят:
оценка рисков+
выбор уровня детализации анализируемых объектов+
наказание за создание уязвимостей

П 10. На межсетевой экран целесообразно возложить функции:
активного аудита+
анализа защищенности
идентификации/аутентификации удаленных пользователей -

П 11. Из принципа разнообразия защитных средств следует, что:
в разных точках подключения корпоративной сети к Internet необходимо устанавливать разные межсетевые экраны
каждую точку подключения корпоративной сети к Internet необходимо защищать несколькими видами средств безопасности+
защитные средства нужно менять как можно чаще

П 12. Программно-технические меры безопасности подразделяются на:
превентивные, препятствующие нарушениям информационной безопасности+
меры обнаружения нарушений+
меры воспроизведения нарушений

П 13. Согласно стандарту X.700, в число функций управления конфигурацией входят:
запуск и остановка компонентов

выбор закупаемой конфигурации
изменение конфигурации системы+

П 14. В число этапов процесса планирования восстановительных работ входят:
идентификация персонала
проверка персонала
идентификация ресурсов +

П 15. В число направлений повседневной деятельности на процедурном уровне входят:
поддержка пользователей+
поддержка программного обеспечения
поддержка унаследованного оборудования

П 16. Что из перечисленного относится к числу основных аспектов информационной безопасности:
подлинность - аутентичность субъектов и объектов
целостность - актуальность и непротиворечивость информации, защищенность информации и поддерживающей инфраструктуры от разрушения и несанкционированного изменения+
стерильность - отсутствие недекларированных возможностей

П 17. В следующих странах сохранилось жесткое государственное регулирование разработки и распространения криптосредств на внутреннем рынке:
Китай+
Россия
Франция +

П 18. Обеспечение высокой доступности можно ограничить:
критически важными серверами
сетевым оборудованием
всей цепочкой от пользователей до серверов +

П 19. Уровень безопасности B, согласно Оранжевой книге, характеризуется:
произвольным управлением доступом
принудительным управлением доступом+
верифицируемой безопасностью

П 20. В следующих странах сохранилось жесткое государственное регулирование разработки и распространения криптосредств на внутреннем рынке:

Китай+
Россия
Франция +

П 21. Обеспечение высокой доступности можно ограничить:
критически важными серверами
сетевым оборудованием
всей цепочкой от пользователей до серверов +

П 22. Информационная безопасность - это дисциплина:
комплексная+
техническая
программистская

П 23. Сервисы безопасности подразделяются на:
глобализующие, расширяющие зону поиска нарушителя
локализующие, сужающие зону воздействия нарушений+
буферизующие, сглаживающие злоумышленную активность

П 24. Политика безопасности:
фиксирует правила разграничения доступа-
отражает подход организации к защите своих информационных активов+
описывает способы защиты руководства организации

П 25. Протоколирование само по себе не может обеспечить неотказуемость, потому что:
регистрационная информация может быть рассредоточена по разным сервисам и разным компонентам распределенной ИС-
целостность регистрационной информации может быть нарушена+
должна соблюдаться конфиденциальность регистрационной информации, а проверка неотказуемости нарушит конфиденциальность

П 26. В число этапов управления рисками входят:
оценка рисков+
выбор уровня детализации анализируемых объектов+
наказание за создание уязвимостей

П 27. На межсетевой экран целесообразно возложить функции:
активного аудита+
анализа защищенности
идентификации/аутентификации удаленных пользователей -

П 28. Из принципа разнообразия защитных средств следует, что:
в разных точках подключения корпоративной сети к Internet необходимо устанавливать разные межсетевые экраны

каждую точку подключения корпоративной сети к Internet необходимо защищать несколькими видами средств безопасности+
защитные средства нужно менять как можно чаще

Критерии оценки для проведения промежуточной аттестации 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 №____