ФГАОУ ВО «Тюменский государственный университет»
Тобольский педагогический институт им. Д.И. Менделеева (филиал)
Тюменского государственного университета

УТВЕРЖДЕНО
Заместителем директора филиала
Шитиковым П.М.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

для обучающихся по направлению подготовки
44.03.05 Педагогическое образование (с двумя профилями подготовки)
профили подготовки
Физическая культура; безопасность жизнедеятельности
формы обучения очная, заочная

1. Паспорт оценочных материалов по дисциплине

№ п/п	Темы дисциплины в ходе текущего контроля, вид промежуточной аттестации	Код и содержание компетенции	Оценочные материалы
1	2	3	4
1.	Информационная безопасность - основные понятия	УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	Защита реферата Опрос по планам практических занятий, выполнение теста №1, ответ на экзамене
2.	Основные угрозы информационной безопасности в информационной образовательной среде	УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач ПК-1 Способен осуществлять обучение учебному предмету на основе использования предметных методик с учетом возрастных и индивидуальных особенностей обучающихся	Защита реферата Опрос по планам практических занятий, выполнение теста №1, ответ на экзамене
3	Основные меры защиты информации в распределенных компьютерных системах	УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач ПК-1 Способен осуществлять обучение учебному предмету на основе использования предметных методик с учетом возрастных и индивидуальных особенностей обучающихся	Защита реферата Опрос по планам практических занятий, выполнение теста №1, ответ на экзамене
4	Взаимодействие в условиях недостоверной информации и ее распределение в среде	УК-1 Способен осуществлять поиск, критический анализ и синтез информации,	Защита реферата Опрос по планам практических занятий, выполнение теста№1, ответ на экзамене

№ п/п	Темы дисциплины в ходе текущего контроля, вид промежуточной аттестации	Код и содержание компетенции	Оценочные материалы
		применять системный подход для решения поставленных задач	
5	Стандарты в области информационной безопасности в ИОС	УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	Защита реферата Опрос по планам практических занятий, выполнение теста №», ответ на экзамене
6	Правовое обеспечение информационной безопасности.	УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	Защита реферата Опрос по планам практических занятий, выполнение теста №2, ответ на экзамене
7	Законодательство в области защиты информации. Компьютерные правонарушения.	УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	Защита реферата Опрос по планам практических занятий, выполнение теста №2, ответ на экзамене
8	Лицензирование и сертификация в информационной среде	УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	Защита реферата Опрос по планам практических занятий, выполнение теста №2, ответ на экзамене
9	Организационное обеспечение информационной безопасности в ИОС	УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	Защита реферата Опрос по планам практических занятий, выполнение теста №2, ответ на экзамене
	Экзамен (7 семестр)	УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач ПК-1 Способен	ответ на экзамене

№ п/п	Темы дисциплины в ходе текущего контроля, вид промежуточной аттестации	Код и содержание компетенции	Оценочные материалы
		осуществлять обучение учебному предмету на основе использования предметных методик с учетом возрастных и индивидуальных особенностей обучающихся	

2. Виды и характеристика оценочных средств

Текущий контроль успеваемости обучающихся включает в себя практические занятия, тесты, рефераты, контрольные работы. На практических занятиях, преподаватель обсуждает с обучающимся поставленные вопросы и выставляет баллы. Практическое занятие также могут проводиться в форме тестирования по тестам разделов дисциплины. Форма проведения промежуточной аттестации по дисциплине –экзамен 7 семестре (ЗФО, ОФО).

Подготовка к практическому занятию. На каждом занятии рассматриваются теоретические вопросы. Обучающийся должен подготовиться к ним и принять участие в обсуждении теоретических вопросов. При подготовке к практическому занятию обучающийся в тетради для практических работ записывает название работы, чертит необходимые графики, таблицы, схемы, рисунки и оставляет место для выводов.

Выполнение рефератов, докладов, сообщений. Обучающийся может по желанию выбрать тему реферата и выступить с докладом на практическом занятии. Материалы реферата могут быть изложены также на лекции как фрагментарно, так и в виде презентации, если преподаватель сочтет это важным и нужным.

Подготовка к тестированию. Задания в тестовой форме используются для проведения контрольной работы. Темы тестовых заданий формулируются по материалу лекционных и практических работ. Индивидуализация теста для обучающихся формируется по вариантам. Преподаватель назначает дату проведения работы и обговаривает тематику. Обучающийся повторяет теоретические вопросы, готовится к контрольной работе.

3. Оценочные средства

Примерные тестовые задания для проведения текущего контроля

Контрольная работа № 1

Наиболее распространенные 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

2. Название информации, которую следует защищать (по нормативам, правилам сети, системы):

а) Регламентированной

б) Правовой

в) Защищаемой

3. Что такое 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
4. 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
5. Что такое источник угрозы?
а) потенциальный злоумышленник
б) злоумышленник
в) нет правильного ответа
6. Что такое окно опасности?
а) промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется.
б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области
в) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере
7. Информационная безопасность:
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
8. 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
9. Информационная безопасность зависит от следующих факторов:
а) компьютеров, поддерживающей инфраструктуры
б) пользователей
в) информации
10. Основные источники внутренних отказов:
а) отступление от установленных правил эксплуатации
б) разрушение данных
в) все ответы правильные
11. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:
а) невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности

б) обрабатывать большой объем программной информации
в) нет правильного ответа
12. Утечка информации в системе — ситуация, характеризуемая:
а) Потерей данных в системе
б) Изменением формы информации
в) Изменением содержания информации
13. Свойством информации, наиболее актуальным при обеспечении информационной безопасности является:
а) Целостность
б) Доступность
в) Актуальность
14. Определите, когда целесообразно не предпринимать никаких действий в отношении выявленных рисков:
а) когда риски не могут быть приняты во внимание по политическим соображениям
б) для обеспечения хорошей безопасности нужно учитывать и снижать все риски
в) когда стоимость контрмер превышает ценность актива и потенциальные потери
15. Что такое политика безопасности?
а) детализированные документы по обработке инцидентов безопасности
б) широкие, высокоуровневые заявления руководства +
в) общие руководящие требования по достижению определенного уровня безопасности
16. Выберите, какая из приведенных техник является самой важной при выборе конкретных защитных мер:
а) анализ рисков
б) результаты ALE
в) анализ затрат / выгоды +
17. Угроза информационной системе (компьютерной сети):
а) Вероятное событие
б) Детерминированное (всегда определенное) событие
в) Событие, происходящее периодически
18. Разновидностями угроз безопасности (сети, системы) являются:
а) Программные, технические, организационные, технологические
б) Серверные, клиентские, спутниковые, наземные
в) Личные, корпоративные, социальные, национальные
19. Окончательно, ответственность за защищенность данных в компьютерной сети несет:
а) Владелец сети
б) Администратор сети
в) Пользователь сети
20. По механизму распространения П.О. различают:
а) вирусы
б) черви
в) все ответы правильные
21. Что такое отказ, ошибки, сбой?
а) случайные угрозы
б) преднамеренные угрозы
в) природные угрозы

22. Определите, что такое отказ:
а) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
б) некоторая последовательность действий, необходимых для выполнения конкретного задания
в) структура, определяющая последовательность выполнения и взаимосвязи процессов
23. Определите, что такое ошибка:
а) неправильное выполнение элементом одной или нескольких функций происходящее в следствии специфического состояния+
б) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
в) негативное воздействие на программу
24. Конфиденциальность это:
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
25. Определите, для чего создаются информационные системы:
а) получения определенных информационных услуг
б) обработки информации
в) оба варианта верны
26. Процедура это:
а) пошаговая инструкция по выполнению задачи
б) обязательные действия
в) руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
27. Определите, какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании:
а) проведение тренингов по безопасности для всех сотрудников
б) поддержка высшего руководства
в) эффективные защитные меры и методы их внедрения
28. Что такое сбой?
а) такое нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент
б) неправильное выполнение элементом одной или нескольких функций происходящее в следствие специфического состояния
в) объект-метод
29. Что такое побочное влияние?
а) негативное воздействие на систему в целом или отдельные элементы+
б) нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент
в) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
30. Относится к человеческому компоненту СЗИ:
а) системные порты

б) администрация

в) программное обеспечение

Контрольная работа № 2

1. Возможность за приемлемое время получить требуемую информационную услугу называется:

1. Конфиденциальность
2. Доступность
3. Целостность
4. Непрерывность

2) К аспектам информационной безопасности не относится:

1. Доступность
2. Целостность
3. Конфиденциальность
4. Защищенность

3) По каким критериям нельзя классифицировать угрозы:

1. по расположению источника угроз
2. по аспекту информационной безопасности, против которого угрозы направлены в первую очередь
3. по способу предотвращения
4. по компонентам информационных систем, на которые угрозы нацелены

4) Главное достоинство парольной аутентификации – …

1. простота
2. надежность
3. секретность
4. запоминаемость

5) Сколько уровней включает в себя сетевая модель OSI?

1. 5
2. 7
3. 6
4. 8

6) Межсетевой экран (Брандмауэр, firewall) – это…

1. Комплекс аппаратных средств
2. Комплекс программных средств
3. Комплекс аппаратных или программных средств
4. Комплекс аппаратных и программных средств

7) На каком уровне сетевой модели OSI не работает межсетевой экран:

1. Физический
2. Сеансовый
3. Сетевой
4. Транспортный

8) Межсетевого экрана какого класса не существует:

1. экранирующий маршрутизатор
2. экранирующий коммутатор
3. экранирующий транспорт
4. экранирующий шлюз

9) Что из перечисленного не входит в состав программного комплекса антивирусной защиты:
   1. Подсистема сканирования
   2. Подсистема управления
   3. Подсистема обнаружения вирусной активности
   4. Подсистема устранения вирусной активности
10) На каком этапе заканчивается жизненный цикл автоматизированной системы?
   1. Бета-тестирование системы
   2. Внедрение финальной версии системы в эксплуатацию
   3. Прекращение сопровождения и технической поддержки системы
   4. Альфа-тестирование системы
11) Какие задачи выполняет теория защиты информации:
   1. предоставлять полные и адекватные сведения о происхождении, сущности и развитии проблем защиты
   2. аккумулировать опыт предшествующего развития исследований, разработок и практического решения задач защиты информации
   3. формировать научно обоснованные перспективные направления развития теории и практики защиты информации
   4. выполняет все вышеперечисленные
12) Какой из протоколов не относится к протоколам защищенной передачи данных в сети Интернет:
   1. SSL
   2. SET
   3. HTTP
   4. IPSec
13) Какого метода разграничения доступа не существует:
   1. разграничение доступа по спискам
   2. разграничение доступа по уровням секретности и категориям
   3. локальное разграничение доступа
   4. парольное разграничение доступа
14) К основным функциям подсистемы защиты операционной системы относятся:
   1. идентификация, аутентификация, авторизация, управление политикой безопасности и разграничение доступа
   2. криптографические функции
   3. сетевые функции
   4. все вышеперечисленные

Темы рефератов

1. Психологические аспекты безопасности в образовании.
2. Информационная безопасность пользователя.
3. Риски и угрозы информационной безопасности. праве.
4. Деструктивные интернет сообщества.
5. Формирование Российского информационного пространства.
6. Национальные интересы в сфере информационной безопасности.
7. Развитие средств защиты информации.
8. Правовое обеспечение информационной безопасности.

9. Очищение информационного поля России.
10. Борьба с фейковыми новостями.
11. Права и обязанности граждан в области информационной безопасности.
12. Целевые программы в сфере информационной безопасности.
13. Организация деятельности по обеспечению информационной безопасности.
14. Органы по обеспечению информационной безопасности.
15. Подготовка нормативной документации о проведении инструктажа сотрудников, организации контроля за соблюдением процедур, связанных с защитой информации.
16. Криптографических средств защиты информации (симметричные и асиммитричные системы шифрования).
17. Основные трудности обеспечения информационной безопасности в настоящее время.
18. Стандарты в области информационной безопасности в ИОС.
19. Основные меры защиты информации в распределенных компьютерных системах.
20. Правила и меры обеспечения информационной безопасности для эффективной организации учебно-воспитательного процесса в школе.

Примерный перечень вопросов для экзамена

1. Понятие информационной безопасности.
2. Аспекты безопасности.
3. Обеспечение безопасности информации.
4. Политика безопасности.
5. Доктрина информационной безопасности Российской Федерации.
6. История и современные проблемы информационной безопасности.
7. Организационно-правовое обеспечение защиты информации.
8. Гуманитарные проблемы информационной безопасности.
9. Политика информационной безопасности (комплексная система защиты).
10. Защита информации от несанкционированного доступа.
11. Уязвимость информации.
12. Программы-вирусы
13. Защита информации от утечки по техническим каналам
14. Определение «уязвимости», «угрозы», «атаки» и «эксплойта».
15. Модели угроз и виды угроз (антропогенные, техногенные, стихийные источники угроз).
16. Модель нарушителя: определение хакерства.
17. Цели и задачи хакера. «Белые», «серые» и «черные» хакеры.
18. Организация режима и охраны.
19. Организация работы с сотрудниками.
20. Организация работы с документами и документированной информацией.
21. Организация использования технических средств сбора, обработки, накопления и хранения конфиденциальной информации.
22. Технические средства защиты информации.
23. Аппаратные средства защиты информации.
24. Программные средства защиты информации.
25. Понятие компьютерного вируса.
26. Классификация компьютерных вирусов.
27. Вредоносные программы.

28. Основные механизмы обеспечения ИБ: идентификация, аутентификация, авторизация, аудит.
29. Конфиденциальная информация и персональные данные.
30. Основные правила антивирусной безопасности.
31. Безопасность в социальных сетях.
32. Криптографические методы защиты информации.
33. Правила безопасности в Интернете для школьников.