ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ИНКЛЮЗИВНОГО ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра информационных технологий и прикладной математики

Утверждаю»
Заведующий кафедрой
Информационных технологий и
прикладной математики
_____ Петрунина Е.В.
«30» 08 2019

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Информационная безопасность в профессиональной деятельности педагога
наименование дисциплины / практики

44.03.02. Психолого-педагогическое образование
шифр и наименование направления подготовки

Психология и педагогика инклюзивного образования
наименование профиля подготовки

Москва 2019

Составитель: МГТЭУ, доцент кафедры ИТиПМ

Белокладов Д.Н. 20.05.2019

Рецензент: МГТЭУ, профессор кафедры ИТиПМ

Истомина Т.В. «21» 05 2019 г.

Согласовано:

Представитель работодателя
или объединения работодателей _____ / Ф.И.О/

Тюсенькова С.Н.

(должность, место работы)

«26» августа 2019 г.

Фонд оценочных средств рассмотрен и одобрен на заседании кафедры ИТиПМ протокол № 1 от «26» 05 2019 г.

Дополнения и изменения, внесенные в фонд оценочных средств, утверждены на заседании кафедры информационных технологий и прикладной математики,
протокол № 1 от «24» 08 2020 г.
Заведующий кафедрой _____ / Ф.И.О/

Дополнения и изменения, внесенные в фонд оценочных средств, утверждены на заседании кафедры _____,
протокол № ____ от «____» _____ 20__ г.
Заведующий кафедрой _____ / Ф.И.О/

Дополнения и изменения, внесенные в фонд оценочных средств, утверждены на заседании кафедры _____,
протокол № ____ от «____» _____ 20__ г.
Заведующий кафедрой _____ / Ф.И.О/

РАССМОТРЕНО
ОДОБРЕНО И
УЧЕБНО-МЕТОДИЧЕСКИМ
СОВЕТОМ МГГУ
ПР.№ 8 30.08 2019 г.

Содержание

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Информационная безопасность в профессиональной деятельности педагога»

Оценочные средства составляются в соответствии с рабочей программой дисциплины и представляют собой совокупность контрольно-измерительных материалов (типовые задачи (задания), контрольные работы, тесты и др.), предназначенных для измерения уровня достижения обучающимися установленных результатов обучения.

Оценочные средства используются при проведении текущего контроля успеваемости и промежуточной аттестации.

Таблица 1 - Перечень компетенций, формируемых в процессе освоения дисциплины

Код компетенции	**Наименование результата обучения**
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
	УК-2.1. Знает необходимые для осуществления профессиональной деятельности правовые нормы и методологические основы принятия управленческого решения. УК-2.2. Умеет анализировать альтернативные варианты решений для достижения намеченных результатов; разрабатывать план, определять целевые этапы и основные направления работ. УК-2.3. Владеет методиками разработки цели и задач проекта; методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах.

Конечными результатами освоения дисциплины являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», расписанные по отдельным компетенциям. Формирование дескрипторов происходит в течение всего семестра по этапам в рамках контактной работы, включающей различные виды занятий и самостоятельной работы, с применением различных форм и методов обучения (табл.2).

Таблица 2 - Формирование компетенций в процессе изучения дисциплины:

Код компетенции	Уровень освоения компетенций	Индикаторы достижения компетенций	Вид учебных занятий[1], работы, формы и методы обучения, способствующие формированию и развитию компетенций[2]	Контролируемые разделы и темы дисциплины[3]	Оценочные средства, используемые для оценки уровня сформированности компетенции[4]
УК-2		*Знает*			
	Недостаточный уровень	УК-2. Студент не способен самостоятельно выделять главные положения в изученном материале дисциплины. Не знает необходимые для осуществления профессиональной деятельности правовые нормы и методологические основы принятия управленческого решения.	Лекционные и практические занятия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета.	1. Введение в информационную безопасность (ИБ). 2. Технологии защиты данных. 3. Технологии защиты вычислительных систем. 4. Технологии обнаружения вторжений. 5. Управление безопасностью.	Текущий контроль – устный опрос, тестирование.

[1] Лекционные занятия, практические занятия, лабораторные занятия, самостоятельная работа…

[2] Необходимо указать активные и интерактивные методы обучения (например, интерактивная лекция, работа в малых группах, методы мозгового штурма и т.д.), способствующие развитию у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств.

[3] Наименование темы (раздела) берется из рабочей программы дисциплины.

[4] Оценочное средство должно выбираться с учетом запланированных результатов освоения дисциплины, например:
«Знать» – собеседование, коллоквиум, тест…
«Уметь», «Владеть» – индивидуальный или групповой проект, кейс-задача, деловая (ролевая) игра, портфолио…

	Базовый уровень	УК-2.1. Студент усвоил основное содержание материала дисциплины, но имеет пробелы в усвоении материала. Имеет несистематизированные знания об основах математики и физики. Показывает слабое знание необходимых для осуществления профессиональной деятельности правовых норм.	Лекционные и практические занятия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета.	1. Введение в информационную безопасность (ИБ). 2. Технологии защиты данных. 3. Технологии защиты вычислительных систем. 4. Технологии обнаружения вторжений. 5. Управление безопасностью.	Текущий контроль – устный опрос, тестирование.
	Средний уровень	УК-2.1. Студент способен самостоятельно выделять главные положения в изученном материале. Знает необходимые для осуществления профессиональной деятельности правовые нормы и методологические основы принятия решений.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета.	1. Введение в информационную безопасность (ИБ). 2. Технологии защиты данных. 3. Технологии защиты вычислительных систем. 4. Технологии обнаружения вторжений. 5. Управление безопасностью.	Текущий контроль – устный опрос, тестирование.
	Высокий уровень	УК-2.1. Студент знает, понимает, выделяет главные положения в изученном материале и способен дать краткую характеристику основным идеям проработанного материала дисциплины. Показывает глубокое знание и понимание необходимых для осуществления профессиональной деятельности правовых норм и методологических основ принятия управленческого решения.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета.	1. Введение в информационную безопасность (ИБ). 2. Технологии защиты данных. 3. Технологии защиты вычислительных систем. 4. Технологии обнаружения вторжений. 5. Управление безопасностью.	Текущий контроль – устный опрос, тестирование.
		Умеет			
	Базовый уровень	УК-2.2. Студент непоследовательно разрабатывает план и основные направления работ.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия,	1. Введение в информационную безопасность (ИБ). 2. Технологии защиты данных. 3. Технологии защиты вычислительных	Текущий контроль – устный опрос, тестирование.

			самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета.	систем. 4. Технологии обнаружения вторжений. 5. Управление безопасностью.	
	Средний уровень	УК-2.2. Студент умеет анализировать альтернативные варианты решений для достижения намеченных результатов; разрабатывать план работ.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета.	1. Введение в информационную безопасность (ИБ). 2. Технологии защиты данных. 3. Технологии защиты вычислительных систем. 4. Технологии обнаружения вторжений. 5. Управление безопасностью.	Текущий контроль – устный опрос, тестирование.
	Высокий уровень	УК-2.2. Студент умеет самостоятельно анализировать альтернативные варианты решений для достижения намеченных результатов; разрабатывать план, определять целевые этапы и основные направления работ.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета.	1. Введение в информационную безопасность (ИБ). 2. Технологии защиты данных. 3. Технологии защиты вычислительных систем. 4. Технологии обнаружения вторжений. 5. Управление безопасностью.	Текущий контроль – устный опрос, тестирование.
		Владеет			
	Базовый уровень	УК-2.3. Студент владеет основными навыками методиками разработки цели и задач проекта.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета.	1. Введение в информационную безопасность (ИБ). 2. Технологии защиты данных. 3. Технологии защиты вычислительных систем. 4. Технологии обнаружения вторжений. 5. Управление безопасностью.	Текущий контроль – устный опрос, тестирование.

	Средний уровень	УК-2.3. Студент владеет методиками разработки цели и задач проекта; методами оценки продолжительности проекта.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета.	1. Введение в информационную безопасность (ИБ). 2. Технологии защиты данных. 3. Технологии защиты вычислительных систем. 4. Технологии обнаружения вторжений. 5. Управление безопасностью.	Текущий контроль – устный опрос, тестирование.
	Высокий уровень	УК-2.3. Студент владеет методиками разработки цели и задач проекта; методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета.	1. Введение в информационную безопасность (ИБ). 2. Технологии защиты данных. 3. Технологии защиты вычислительных систем. 4. Технологии обнаружения вторжений. 5. Управление безопасностью.	Текущий контроль – устный опрос, тестирование.

2. ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ[5]

Таблица 3

№	Наименование оценочного средства	Характеристика оценочного средства	Представление оценочного средства в ФОС
1	Устный опрос	Средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования преподавателя с обучающимися.	Вопросы по темам/разделам дисциплины
2	Тест	Средство, позволяющее оценить уровень знаний обучающегося путем выбора им одного из нескольких вариантов ответов на поставленный вопрос. Возможно использование тестовых вопросов, предусматривающих ввод обучающимся короткого и однозначного ответа на поставленный вопрос.	Тестовые задания

[5] Указываются оценочные средства, применяемые в ходе реализации рабочей программы данной дисциплины.

3. ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ

Оценивание результатов обучения по дисциплине «Информационная безопасность в профессиональной деятельности педагога» осуществляется в соответствии с Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся.

Предусмотрены следующие виды контроля: текущий контроль (осуществление контроля всех видов аудиторной и внеаудиторной деятельности обучающегося с целью получения первичной информации о ходе усвоения отдельных элементов содержания дисциплины) и промежуточная аттестация (оценивается уровень и качество подготовки по дисциплине в целом).

Показатели и критерии оценивания компетенций, формируемых в процессе освоения данной дисциплины, описаны в табл. 4.

Таблица 4.

Код компетенции	Уровень освоения компетенции	Индикаторы достижения компетенции	Критерии оценивания результатов обучения
УК-2		Знает	
	Недостаточный уровень Оценка «незачтено»	*УК-2.1.*	*Не знает значительной части материала курса, не способен самостоятельно выделять главные положения в изученном материале дисциплины*
	Базовый уровень Оценка, «зачтено»	*УК-2.1.*	*Знает не менее 50 % основного материала курса, однако испытывает затруднения в его применении*
	Средний уровень Оценка «зачтено»	*УК-2.1.*	*Знает основную часть материала курса, способен применить изученный материал на практике, испытывает незначительные затруднения в решении задач*
	Высокий уровень Оценка «зачтено»	*УК-2.1.*	*Показывает глубокое знание и понимание материала, способен применить изученный материал на практике*
		Умеет	
	Базовый уровень	*УК-2.2.*	*Умеет воспроизвести не менее 50 % основного материала курса, однако испытывает затруднения при решении практических задач*
	Средний уровень	*УК-2.2.*	*Умеет решать стандартные профессиональные задачи с применением полученных знаний, испытывает незначительные затруднения в решении задач*
	Высокий уровень	*УК-2.2.*	*Умеет решать стандартные профессиональные задачи с применением полученных знаний, показывает глубокое знание и понимание материала, способен решить задачу при изменении формулировки*
		Владеет	
	Базовый уровень	*УК-2.3.*	*Владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности, усвоил основное содержание материала дисциплины,*

			но имеет пробелы в усвоении материала. Имеет несистематизированные знания основных разделов дисциплины.
	Средний уровень	*УК-2.3.*	*Владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности, способен самостоятельно выделять главные положения в изученном материале. Испытывает незначительные затруднения в решении задач.*
	Высокий уровень	*УК-2.3.*	*Свободно владеет навыками теоретического и экспериментального исследования, показывает глубокое знание и понимание изученного материала*

4. Методические материалы, определяющие процедуры оценивания результатов обучения

Задания в форме устного опроса:

Устный опрос используется для текущего контроля успеваемости обучающихся по дисциплине в качестве проверки результатов освоения терминологии. Каждому студенту выдается свой собственный, узко сформулированный вопрос. Ответ должен быть четким и кратким, содержащим все основные характеристики описываемого понятия, института, категории.

Задания в форме тестирования

Тест представляет собой контрольное мероприятие по учебному материалу каждой темы (раздела) дисциплины, состоящее в выполнении обучающимся системы стандартизированных заданий, которая позволяет автоматизировать процедуру измерения уровня знаний и умений обучающегося.

Тестирование является средством текущего контроля успеваемости обучающихся по дисциплине и может включать в себя следующие типы заданий: задание с единственным выбором ответа из предложенных вариантов, задание на определение верных и неверных суждений; задание с множественным выбором ответов.

В каждом задании необходимо выбрать все правильные ответы.

5. Материалы для проведения текущего контроля и промежуточной аттестации

Задания в форме устного опроса

Семестр 4

1. Введение в информационную безопасность (ИБ)
2. Основные понятия ИБ.
3. Анализ угроз.
4. Проблемы безопасности компьютерных сетей.
5. Политика безопасности.
6. Основные составляющие политики безопасности.
7. Нормативно-правовое обеспечение ИБ.
8. Стандарты ИБ.
9. Международные стандарты в сфере ИБ.
10. Принципы защиты информационных систем (ИС).
11. Технологии защиты данных.
12. Принципы криптозащиты.
13. Криптографические алгоритмы.
14. Криптоанализ.
15. Симметричные и асимметричные системы шифрования.
16. Технологии электронно-цифровой подписи.
17. Функции хэширования.
18. Технологии аутентификации.
19. Биометрическая аутентификация.
20. Технологии защиты вычислительных систем.
21. Обеспечение безопасности операционных систем (ОС).
22. Межсетевые экраны.
23. Сертификация и стандартизация.
24. Защита в виртуальных сетях VPN.
25. Защита на уровнях модели OSI.
26. Технологии обнаружения вторжений.
27. Средство анализа сетевого трафика Wireshark.
28. Сканирование сети.
29. Анализ защищенности.
30. Обнаружение атак.
31. Программные средства обнаружения вторжения.
32. Защита удаленного доступа.
33. Защита от вирусов и спама.
34. Управление безопасностью.
35. Задачи управления ИБ в информационных системах (ИС).
36. Архитектура и функционирование систем управления ИБ в (ИС).
37. Аудит и мониторинг безопасности (ИС).
38. Обзор систем управления безопасностью.

Контролируемые компетенции: УК-2.
Оценка компетенций осуществляется в соответствии с таблицей 4.

Тестовые задания

Семестр 4

1. Кто является основным ответственным за определение уровня классификации информации?

Руководитель среднего звена
Высшее руководство
Владелец
Пользователь

2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

Сотрудники
Хакеры
Атакующие
Контрагенты (лица, работающие по договору)

3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
Улучшить контроль за безопасностью этой информации
Снизить уровень классификации этой информации

4. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

Поддержка высшего руководства
Эффективные защитные меры и методы их внедрения
Актуальные и адекватные политики и процедуры безопасности
Проведение тренингов по безопасности для всех сотрудников

5. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
Когда риски не могут быть приняты во внимание по политическим соображениям
Когда необходимые защитные меры слишком сложны
Когда стоимость контрмер превышает ценность актива и потенциальные потери

6. Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?

Только военные имеют настоящую безопасность
Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности
Военным требуется больший уровень безопасности, т.к. их риски существенно выше
Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности

7. Защита информации от утечки – это деятельность по предотвращению:

получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;

воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;

воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;

неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;

несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

8. Защита информации это:

процесс сбора, накопления, обработки, хранения, распределения и поиска информации;

преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;

получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;

совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;

деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

9. Естественные угрозы безопасности информации вызваны:

деятельностью человека;

ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;

воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;

корыстными устремлениями злоумышленников;

ошибками при действиях персонала.

10. Искусственные угрозы безопасности информации вызваны:

деятельностью человека;

ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;

воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;

корыстными устремлениями злоумышленников;

ошибками при действиях персонала.

11. К основным непреднамеренным искусственным угрозам АСОИ относится:

физическое разрушение системы путем взрыва, поджога и т.п.;

перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;

изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;

чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы.

12. К посторонним лицам нарушителям информационной безопасности относится:

представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;

персонал, обслуживающий технические средства;

технический персонал, обслуживающий здание;

пользователи;

сотрудники службы безопасности.

представители конкурирующих организаций.

лица, нарушившие пропускной режим;

13. Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п:

черный пиар;

фишинг;

нигерийские письма;

источник слухов;

пустые письма.

14. Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:

черный пиар;

фишинг;

нигерийские письма;

источник слухов;

пустые письма.

15. Активный перехват информации - это перехват, который:

заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;

основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;

неправомерно использует технологические отходы информационного процесса;

осуществляется путем использования оптической техники;

осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

16. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:

активный перехват;

пассивный перехват;

аудиоперехват;

видеоперехват;

просмотр мусора.

17. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:
- активный перехват;
- пассивный перехват;
- аудиоперехват;
- видеоперехват;
- просмотр мусора.

18. Перехват, который осуществляется путем использования оптической техники называется:
- активный перехват;
- пассивный перехват;
- аудиоперехват;
- видеоперехват;
- просмотр мусора.

19. Степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования — это
- уязвимость информации
- надежность информации
- защищенность информации
- безопасность информации

20. Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы — это
- аудит
- аутентификация
- авторизация
- идентификация

21. Совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности в соответствии с ее назначением, называется
- актуальностью информации
- доступностью
- качеством информации
- целостностью

22. Первым этапом разработки системы защиты ИС является
- анализ потенциально возможных угроз информации
- изучение информационных потоков
- стандартизация программного обеспечения
- оценка возможных потерь

23. Надежность системы защиты информации определяется
- усредненным показателем
- самым слабым звеном
- количеством отраженных атак
- самым сильным звеном

24. Политика информационной безопасности — это
- профиль защиты

итоговый документ анализа рисков
стандарт безопасности
совокупность законов, правил, определяющих управленческие и проектные решения в области защиты информации

25. Присвоение субъектам и объектам доступа уникального номера, шифра, кода и т.п. с целью получения доступа к информации — это
аутентификация
идентификация
аудит
авторизация

26. Какой тип воздействия осуществляет программная закладка, которая внедряется в ПЗУ, системное или прикладное программное обеспечение и сохраняет всю или выбранную информацию в скрытой области памяти:
компрометация
перехват
наблюдение
уборка мусора

27. Содержанием параметра угрозы безопасности информации «конфиденциальность» является
несанкционированная модификация
искажение
несанкционированное получение
уничтожение

28. Требования к техническому обеспечению системы защиты:
аппаратурные и физические
управленческие и документарные
процедурные и раздельные
административные и аппаратурные

29. Цель процесса внедрения и тестирования средств защиты —
определить уровень расходов на систему защиты
выявить нарушителя
гарантировать правильность реализации средств защиты
выбор мер и средств защиты

30. Возможность получения необходимых пользователю данных или сервисов за разумное время характеризует свойство
восстанавливаемость
детермированность
целостность
доступность

31. Троянские программы — это
программы-вирусы, которые распространяются самостоятельно
все программы, содержащие ошибки
часть программы с известными пользователю функциями, способная выполнять действия с целью причинения определенного ущерба
текстовые файлы, распространяемые по сети

32. Наиболее надежным механизмом для защиты содержания сообщений является
специальный аппаратный модуль
специальный режим передачи сообщения
дополнительный хост
криптография

33. Основной целью системы брандмауэра является управление доступом
к архивам
внутри защищаемой сети
к секретной информации
к защищаемой сети

34. Процесс имитации хакером дружественного адреса называется
«крэком»
проникновением
взломом
«спуфингом»

35. Предоставление легальным пользователем дифференцированных прав доступа к ресурсам системы — это
идентификация
аудит
аутентификация
авторизация

36. Проверка подлинности пользователя по предъявленному им идентификатору — это
авторизация
аутентификация
аудит
идентификация

37. Свойство, которое гарантирует, что информация не может быть доступна или раскрыта для неавторизованных личностей, объектов или процессов — это
детерминированность
достоверность
целостность
конфиденциальность

38. Система, позволяющая разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов из одной части в другую, называется
брандмауэром
браузером
маршрутизатором
фильтром

39. Компьютерным вирусом называется:
любая программа, созданная на языках низкого уровня
небольшая программа, способная к самокопированию, которая может приписывать себя к другим программам
файл, содержащий макросы

нет правильного ответа

40. Что из нижеперечисленного является одним из способов защиты информации на компьютере?
защита паролем данных
дефрагментация жесткого диска
полное отключение системного блока
переустановка операционной системы
нет правильного ответа
все ответы правильные

41. Что такое руткит?
вредоносная программа, отслеживающая, какие сайты посещает пользователь
программа, блокирующая доступ к компьютеру и требующая деньги за разблокировку
программа для скрытого взятия под контроль взломанной системы
нет правильного ответа
все ответы верны

42. Под фишингом понимают
рассылки от имени популярных компаний или организаций, содержащих ссылки на ложные сайты, внешне неотличимые от настоящих.
перераспределение файлов и логической структуры диска
преобразование информации в целях скрытия от неавторизованных лиц
нет правильного ответа
все ответы верны

43. Как называется информация, круг лиц, имеющих доступ к которой ограничен?
открытая
конфиденциальная
зашифрованная

44. Шифрование информации это - ...
преобразование информации, при котором содержание становится непонятным для не обладающих соответствующими полномочиями субъектов
преобразование информации в двоичный код
процесс сжатия информации, с целью уменьшения занимаемого ей объема на диске
все ответы верны
нет правильного ответа

45. Что называют защитой информации?
предотвращение утечки информации
предотвращение несанкционированных действий
предотвращение непреднамеренных воздействий на защищаемую информацию
все ответы верны

46. Что понимают под утечкой информации?
бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена.
преднамеренная порча или уничтожение информации
преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к данным.

Контролируемые компетенции: УК-2.
Оценка компетенций осуществляется в соответствии с таблицей 4.

Темы курсовых работ

Не предусмотрено

Вопросы к зачету

Семестр 4

1. Основные понятия защиты информации и информационной безопасности
2. Анализ угроз информационной безопасности
3. Анализ угроз сетевой безопасности.
4. Способы обеспечения информационной безопасности
5. Основные понятия политики безопасности.
6. Структура политики безопасности организации. Процедуры безопасности
7. Разработка политики безопасности.
8. Стандарты информационной безопасности
9. Основные понятия криптографической защиты информации
10. Симметричные криптосистемы шифрования
11. Асимметричные криптосистемы шифрования
12. Комбинированная криптосистема шифрования
13. Электронная цифровая подпись и функция хэширования
14. Управление криптоключами
15. Аутентификация, авторизация и администрирование действий пользователей
16. Безопасность КИС.
17. Безопасность облачных вычислений.
18. Обеспечение безопасности ОС.
19. Функции межсетевых экранов
20. Особенности функционирования
21. Схемы сетевой защиты на базе МЭ
22. Концепция построения виртуальных защищенных сетей VPN
23. VPN-решения для построения защищенных сетей
24. Протоколы формирования защищенных каналов на канальном уровне
25. Протоколы формирования защищенных каналов на сеансовом уровне
26. Защита беспроводных сетей
27. Архитектура средств безопасности IPSec. Защита передаваемых данных с помощью протоколов AH и ESP
28. Протокол управления криптоключами IKE
29. Основные схемы применения IPSec. Преимущества средств безопасности IPSec
30. Управление идентификацией и доступом
31. Организация защищенного удаленного доступа. Централизованный контроль удаленного доступа
32. Управление доступом по схеме однократного входа с авторизацией Single Sign-On (SSO)
33. Протокол Kerberos
34. Инфраструктура управления открытыми ключами PKI
35. Технология анализа защищенности

36. Технологии обнаружения атак
37. Компьютерные вирусы и проблемы антивирусной защиты.
38. Концепция адаптивного управления безопасностью.

Вопросы к экзамену

Не предусмотрено