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

КАФЕДРА Информационных технологий и прикладной математики

«Утверждаю»

Зав. кафедрой

Информационных технологий и прикладной математики

Петрушина Е.В. «27» августа 2018

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

## Информационная безопасность в деятельности педагога

образовательная программа направления подготовки
44.03.02 Психолого-педагогическое образование

**Профиль подготовки**

«Психология и педагогика инклюзивного образования»
Квалификация (степень) выпускника

Бакалавр

Москва
2018

Составитель / составители: Белоглазов А.А.

Фонд оценочных средств рассмотрен и одобрен на заседании кафедры педагогики и психологии
протокол № 1 от «27» августа 2018 г.
Заведующий кафедрой Петрунина Е.Н. /Ф.И.О/

Дополнения и изменения, внесенные в фонд оценочных средств, утверждены на заседании
кафедры прикладной математики и информатики,
протокол № 1 от «26» августа 2019 г.
Заведующий кафедрой Петрунина Е. Н. / Ф.И.О/

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

Дополнения и изменения, внесенные в фонд оценочных средств, утверждены на заседании
кафедры _____,
протокол № ____ от «____» _____ 201 г.
Заведующий кафедрой _____ / Ф.И.О/

Дополнения и изменения, внесенные в фонд оценочных средств, утверждены на заседании
кафедры _____,
протокол № ____ от «____» _____ 201_ г.
Заведующий кафедрой _____ / Ф.И.О/

РАССМОТРЕНО
ОДОБРЕНО НА
УЧЕБНО-МЕТОДИЧЕСКИМ
СОВЕТОМ МГГЭУ
ПРОТОКОЛ № 8 «31» 08 2018.

Содержание

# 1. Паспорт фонда оценочных средств

по дисциплине «Информационная безопасность в деятельности педагога»

Таблица 1.

| № п/п | Контролируемые разделы (темы), дисциплины[1] | Коды компетенций | Оценочные средства - наименование | |
|---|---|---|---|---|
| | | | текущий контроль | промежуточная аттестация |
| | *7 семестр* | | | |
| 1 | **Тема 1.** Введение в информационную безопасность (ИБ) | ОК-7<br>ПК-28<br>ПК-29 | Устный опрос, тестирование | *вопросы к зачету* |
| 2. | **Тема 2.** Технологии защиты данных | ОК-7<br>ПК-28<br>ПК-29 | Устный опрос, тестирование | *вопросы к зачету* |
| 3. | **Тема 3.** Технологии защиты вычислительных систем | ОК-7<br>ПК-28<br>ПК-29 | Устный опрос, тестирование | *вопросы к зачету* |
| 4. | **Тема 4.** Технологии обнаружения вторжений | ОК-7<br>ПК-28<br>ПК-29 | Устный опрос, тестирование | *вопросы к зачету* |
| 5. | **Тема 5.** Управление безопасностью | ОК-7<br>ПК-28<br>ПК-29 | Устный опрос, тестирование | *вопросы к зачету / Зачет* |

Таблица 2.

Перечень компетенций:

| Код компетенции | Содержание компетенции |
|---|---|
| ОК-7 | Способность к самоорганизации и самообразованию |
| ПК-28 | Способность формировать психологическую готовность будущего специалиста к профессиональной деятельности |
| ПК-29 | Готовность руководить проектно-исследовательской деятельностью обучающихся |

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

## 2. Перечень оценочных средств[2]

**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 |
| 3 | Зачет | | Вопросы к зачету |

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

# 3. Описание показателей и критериев оценивания результатов обучения на различных этапах формирования компетенций

При проведении текущего контроля успеваемости студентов по учебной дисциплине Б1.В.ДВ.14.01 «Информационная безопасность в деятельности педагога» используются следующие критерии оценок:

### 3.1. Критерии оценки 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.

**Описание критериев и шкалы оценивания тестирования**

| Критерий оценивания | Оценка |
|---|---|
| Выставляется обучающемуся при правильных ответах на 80-100% тестов | Отлично |
| Выставляется обучающемуся при правильных ответах на 60-79% тестов. | Хорошо |
| Выставляется обучающемуся при правильных ответах на 50-59% тестов. | Удовлетворительно |
| Выставляется обучающемуся, если правильно даны ответы менее чем на 50% тестов. | Неудовлетворительно |

### 3.2. Критерии оценки 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.

**Описание критериев и шкалы оценивания устного опроса**

| Критерий оценивания | Оценка |
|---|---|
| Выставляется обучающемуся, который подготовил ответ на предложенный вопрос, активно участвует в дискуссии, высказывает собственное мнение, представляет наглядный материал | Отлично |

| | |
|---|---|
| Выставляется обучающемуся, который подготовил ответ на предложенный вопрос, но неактивном участии в дискуссии | Хорошо |
| Выставляется обучающемуся, который частично подготовил ответ на предложенный вопрос, неактивно участвовал в дискуссии | Удовлетворительно |
| Выставляется обучающемуся в случае его неготовности к занятию | Неудовлетворительно |

### 3.3. Критерии оценки зачета (зачета с оценкой)

В ходе ответа обучающийся должен показать сформированность компетенции (или компетенций) по дисциплине.

Результаты ответа определяются оценками «зачтено (отлично)», «зачтено (хорошо)», «зачтено (удовлетворительно)», «незачтено (неудовлетворительно)».

Зачет с оценкой представляет собой форму промежуточного контроля знаний по дисциплине. Он проводится в устной форме. Каждому обучающемуся выдается два теоретических вопроса и одна задача.

На подготовку обучающемуся отводится 30 минут.

**Описание критериев и шкалы оценивания зачета (зачета с оценкой)**

| **Показатели** | **Максимальная оценка в баллах** |
|---|---|
| 1-й вопрос | 30 |
| 2-й вопрос | 30 |
| Задача | 40 |

| 0-50 баллов | 51-70 | 71-85 | 86-100 |
|---|---|---|---|
| Незачтено (неудовлетворительно) | Зачтено (удовлетворительно) | Зачтено (хорошо) | Зачтено (отлично) |

Для оценки уровня освоения дисциплин, профессиональных модулей (их составляющих) устанавливаются следующее соответствие:
«отлично» - высокий уровень освоения;
«хорошо», «удовлетворительно» - достаточный уровень освоения;
«неудовлетворительно» - низкий уровень освоения.

**Таблица 4.**

| Код компетенции | Уровень освоения компетенции | Показатели достижения компетенции | Критерии оценивания результатов обучения |
|---|---|---|---|
| | | Знает | |
| ОК-7 | Недостаточный уровень. Оценка «незачтено» | ОК-7. З-1. | Не знает значительной части материала курса, не способен самостоятельно выделять главные положения в изученном материале дисциплины |
| | Базовый уровень. Оценка «зачтено» | | Знает не менее 50 % основного материала курса, однако испытывает затруднения в его применении |
| | Средний уровень. Оценка «зачтено» | | Знает основную часть материала курса, способен применить изученный материал на практике, испытывает незначительные затруднения в решении задач |
| | Высокий уровень. Оценка «зачтено» | | Показывает глубокое знание и понимание материала, способен применить изученный материал на практике |
| | | Умеет | |
| | Базовый уровень | ОК-7. У-1. | Умеет воспроизвести не менее 50 % основного материала курса, однако испытывает затруднения при решении практических задач |
| | Средний уровень | | Умеет решать стандартные профессиональные задачи с применением полученных знаний, испытывает незначительные затруднения в решении задач |
| | Высокий уровень | | Умеет решать стандартные профессиональные задачи с применением полученных знаний, показывает глубокое знание и понимание материала, способен решить задачу при изменении формулировки |
| | | Владеет | |
| | Базовый уровень | ОК-7. В-1. | 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 | | 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 | | Свободно владеет навыками теоретического и экспериментального исследования, показывает глубокое знание и понимание изученного материала |

| | | | |
|---|---|---|---|
| ПК-28 | | Знает | |
| | Недостаточный уровень. Оценка «незачтено» | ПК-28. З-1. | Не знает значительной части материала курса, не способен самостоятельно выделять главные положения в изученном материале дисциплины |
| | Базовый уровень. Оценка «зачтено» | | Знает не менее 50 % основного материала курса, однако испытывает затруднения в его применении |
| | Средний уровень. Оценка «зачтено» | | Знает основную часть материала курса, способен применить изученный материал на практике, испытывает незначительные затруднения в решении задач |
| | Высокий уровень. Оценка «зачтено» | | Показывает глубокое знание и понимание материала, способен применить изученный материал на практике |
| | | Умеет | |
| | Базовый уровень | ПК-28. У-1. | Умеет воспроизвести не менее 50 % основного материала курса, однако испытывает затруднения при решении практических задач |
| | Средний уровень | | Умеет решать стандартные профессиональные задачи с применением полученных знаний, испытывает незначительные затруднения в решении задач |
| | Высокий уровень | | Умеет решать стандартные профессиональные задачи с применением полученных знаний, показывает глубокое знание и понимание материала, способен решить задачу при изменении формулировки |
| | | Владеет | |
| | Базовый уровень | ПК-28. В-1. | 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 | | 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 | | Свободно владеет навыками теоретического и экспериментального исследования, показывает глубокое знание и понимание изученного материала |
| ПК-29 | | Знает | |
| | Недостаточный уровень. Оценка «незачтено» | ПК-29. З-1. | Не знает значительной части материала курса, не способен самостоятельно выделять главные положения в изученном материале дисциплины |

| | | | |
|---|---|---|---|
| | Базовый уровень. Оценка «зачтено» | | Знает не менее 50 % основного материала курса, однако испытывает затруднения в его применении |
| | Средний уровень. Оценка «зачтено» | | Знает основную часть материала курса, способен применить изученный материал на практике, испытывает незначительные затруднения в решении задач |
| | Высокий уровень. Оценка «зачтено» | | Показывает глубокое знание и понимание материала, способен применить изученный материал на практике |
| | | Умеет | |
| | Базовый уровень | ПК-29. У-1. | Умеет воспроизвести не менее 50 % основного материала курса, однако испытывает затруднения при решении практических задач |
| | Средний уровень | | Умеет решать стандартные профессиональные задачи с применением полученных знаний, испытывает незначительные затруднения в решении задач |
| | Высокий уровень | | Умеет решать стандартные профессиональные задачи с применением полученных знаний, показывает глубокое знание и понимание материала, способен решить задачу при изменении формулировки |
| | | Владеет | |
| | Базовый уровень | ПК-29. В-1. | 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 | | 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 | | Свободно владеет навыками теоретического и экспериментального исследования, показывает глубокое знание и понимание изученного материала |

## 4. Методические материалы, определяющие процедуры оценивания результатов обучения

По видам заданий приводится описание того, каким образом необходимо выполнить данное задание, способы и механизмы его выполнения, выбор номера варианта и др. Примеры методических материалов, определяющих процедуру оценивания результатов обучения, характеризующих этапы формирования компетенций:

- Кейсовые технологии как средство формирования компетенций
- Методические указания по разработке оценочных средств
- Разработка и применение деловых игр
- Иные методические материалы, определяющие процедуры оценивания результатов обучения в ходе реализации рабочей программы дисциплины

### 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 7**

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: ОК-7, ПК-28, ПК-29**
**Оценка компетенций осуществляется в соответствии с Таблицей 4.**

## Задания в форме тестирования

**Семестр 7**

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. Трояские 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: ОК-7, ПК-28, ПК-29**
**Оценка компетенций осуществляется в соответствии с Таблицей 4.**

## Вопросы к зачету

### Семестр 7

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.