МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ПЕРМСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
СГПИ филиал ПГНИУ

Фонды оценочных средств по дисциплине

# «БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ»

Специальность 09.02.06 Сетевое и системное администрирование

**Кодификатор проверяемых элементов содержания**

| Код компетенции | Наименование компетенции | Планируемые результаты обучения | Номер задания |
|---|---|---|---|
| **ОК.1** | Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам | **Знать:** методы и средства защиты компьютерной информации, криптографические методы информационной безопасности. **Уметь:** выбирать способы решения задач профессиональной деятельности применительно к различным контекстам. | **11, 19** |
| **ОК.2** | Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности | **Знать:** основные понятия и определения, используемые при изучении информационной безопасности. **Уметь:** использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности. | **1, 17** |
| **ОК.3** | Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях | **Знать:** методы и способы решения профессиональных задач в области обеспечения информационной безопасности компьютерных сетей. **Уметь:** планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях. | **3, 12** |
| **ОК.4** | Эффективно взаимодействовать и работать в коллективе и команде | **Знать:** концепцию защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. **Уметь:** эффективно взаимодействовать и работать в коллективе и команде. | **4, 13** |
| **ОК.5** | Осуществлять устную и письменную коммуникацию на государственном языке Российской | **Знать:** особенности современных информационных технологий. **Уметь:** осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей | **2, 15** |

| | | | |
|---|---|---|---|
| | Федерации с учетом особенностей социального и культурного контекста | социального и культурного контекста. | |
| **ОК.6** | Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения | **Знать:** нормы и требования российского законодательства в области лицензирования и сертификации, классификацию автоматизированных систем, согласно руководящим документам.<br>**Уметь:** проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения. | **10, 13** |
| **ОК.7** | Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях | **Знать:** классификацию пользователей и злоумышленников в сети Интернет, причины уязвимости сети Интернет; основные понятия и определения, используемые при изучении информационной безопасности.<br>**Уметь:** содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях. | **3, 19** |
| **ОК.8** | Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической | **Знать:** классификацию «компьютерных вирусов», и какую угрозу они представляют для безопасности информации.<br>**Уметь:** использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности. | **9, 20** |

| | | | |
|---|---|---|---|
| | подготовленности | | |
| **ОК.9** | Пользоваться профессиональной документацией на государственном и иностранном языках | **Знать:** состав мероприятий по защите персональных данных.<br>**Уметь:** пользоваться профессиональной документацией на государственном и иностранном языках. | **6, 14** |
| **ПК.1.1** | Документировать состояния инфо-коммуникационных систем и их составляющих в процессе наладки и эксплуатации | **Знать:** виды угроз и методы защиты персональных компьютеров, серверов и корпоративных сетей от них, основные процедуры административного управления.<br>**Уметь:** документировать состояния инфо-коммуникационных систем и их составляющих в процессе наладки и эксплуатации. | **4, 18** |
| **ПК.1.2** | Поддерживать работоспособность аппаратно-программных средств устройств инфо-коммуникационных систем | **Знать:** правила защиты от «компьютерных вирусов», определение аутентификации и разрешения.<br>**Уметь:** поддерживать работоспособность аппаратно-программных средств устройств инфо-коммуникационных систем. | **7, 14** |
| **ПК.1.3** | Устранять неисправности в работе инфо-коммуникационных систем | **Знать:** виды нападений на политику безопасности, основные методы обеспечения безопасности.<br>**Уметь:** устранять неисправности в работе инфо-коммуникационных систем. | **8, 16** |
| **ПК.1.4** | Проводить приемо-сдаточные испытания компьютерных сетей и сетевого оборудования различного уровня и оценку качества сетевой топологии в рамках своей ответственности | **Знать:** классификацию «компьютерных вирусов», методы и средства защиты компьютерной информации.<br>**Уметь:** проводить приемосдаточные испытания компьютерных сетей и сетевого оборудования различного уровня и оценку качества сетевой топологии в рамках своей ответственности. | **8, 14** |
| **ПК.1.5** | Осуществлять резервное копирование и восстановление конфигурации сетевого оборудования информационно-коммуникационных систем | **Знать:** особенности защиты информации в компьютерных сетях.<br>**Уметь:** осуществлять резервное копирование и восстановление конфигурации сетевого оборудования информационно-коммуникационных систем. | **5, 11** |
| **ПК.1.6** | Осуществлять инвентаризацию | **Знать:** особенности защиты в операционных системах. | **7, 15** |

| | | | |
|---|---|---|---|
| | технических средств сетевой инфраструктуры, контроль оборудования после проведенного ремонта | **Уметь:** осуществлять инвентаризацию технических средств сетевой инфраструктуры, контроль оборудования после проведенного ремонта. | |
| **ПК.1.7** | 1.7 Осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфо-коммуникационных систем | **Знать:** алгоритмы работы «компьютерных вирусов» и пути их внедрения в систему.<br>**Уметь:** осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфо-коммуникационных систем. | **6, 12** |

**Вариант 1**

**Задание 1**

1. Основная масса угроз информационной безопасности приходится на:

а) Троянские программы

б) Шпионские программы

в) Черви

г) нет правильного ответа

**Ответ: а**

**Задание 2**

Какой вид идентификации и аутентификации получил наибольшее распространение:

а) системы PKI

б) постоянные пароли

в) одноразовые пароли

г) нет правильного ответа

**Ответ: б**

**Задание 3**

Под какие системы распространение вирусов происходит наиболее динамично:

а) Windows

б) Mac OS

в) Android

г) нет правильного ответа

**Ответ: в**

**Задание 4**

Заключительным этапом построения системы защиты является:

а) сопровождение

б) планирование

в) анализ уязвимых мест

г) нет правильного ответа

**Ответ: а**

**Задание 5**

Какие угрозы безопасности информации являются преднамеренными:
а) ошибки персонала
б) открытие электронного письма, содержащего вирус
в) не авторизованный доступ
г) нет правильного ответа

**Ответ: в**

**Задание 6**

Какой подход к обеспечению безопасности имеет место:
а) теоретический
б) комплексный
в) логический
г) нет правильного ответа

**Ответ: б**

**Задание 7**

Системой криптографической защиты информации является:
а) BFox Pro
б) CAudit Pro
в) Крипто Про
г) нет правильного ответа

**Ответ: в**

**Задание 8**

Какие вирусы активизируются в самом начале работы с операционной системой:
а) загрузочные вирусы
б) троянцы
в) черви
г) нет правильного ответа

**Ответ: а**

**Задание 9**

Stuxnet – это:
а) троянская программа
б) макровирус
в) промышленный вирус
г) нет правильного ответа

**Ответ: в**

**Задание 10**

Таргетированная атака – это:
а) атака на сетевое оборудование
б) атака на компьютерную систему крупного предприятия
в) атака на конкретный компьютер пользователя
г) нет правильного ответа

**Ответ: б**

**Задание 11**

Под информационной безопасностью понимается:

а) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре

б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия

в) нет верного ответа

г) все ответы правильные

**Ответ: а**

**Задание 12**

Защита информации:

а) небольшая программа для выполнения определенной задачи

б) комплекс мероприятий, направленных на обеспечение информационной безопасности

в) процесс разработки структуры базы данных в соответствии с требованиями пользователей

г) нет правильного ответа

**Ответ: б**

**Задание 13**

Информационная безопасность зависит от:

а) компьютеров, поддерживающей инфраструктуры

б) пользователей

в) информации

г) нет правильного ответа

**Ответ: а**

**Задание 14**

Конфиденциальностью называется:

а) защита программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов

б) описание процедур

в) защита от несанкционированного доступа к информации

г) нет правильного ответа

**Ответ: в**

**Задание 15**

Для чего создаются информационные системы:

а) получения определенных информационных услуг

б) обработки информации

в) оба варианта верны

г) нет правильного ответа

**Ответ: а**

**Задание 16**

Кто является основным ответственным за определение уровня классификации информации:

а) руководитель среднего звена

б) владелец

в) высшее руководство

г) нет правильного ответа

**Ответ: б**

**Задание 17**

Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности:

а) хакеры

б) контрагенты

в) сотрудники

г) нет правильного ответа

**Ответ: в**

**Задание 18**

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

а) снизить уровень классификации этой информации

б) улучшить контроль за безопасностью этой информации

в) требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации

г) нет правильного ответа

**Ответ: б**

**Задание 19**

Что самое главное должно продумать руководство при классификации данных:

а) управление доступом, которое должно защищать данные

б) оценить уровень риска и отменить контрмеры

в) необходимый уровень доступности, целостности и конфиденциальности

г) нет правильного ответа

**Ответ: в**

**Задание 20**

Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены:

а) владельцы данных

б) руководство

в) администраторы

г) нет правильного ответа

**Ответ: б**

**Вариант 2**

**Задание 1**

Процедурой называется:

а) пошаговая инструкция по выполнению задачи

б) обязательные действия

в) руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах

г) нет правильного ответа

**Ответ: а**

**Задание 2**

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
г) нет правильного ответа

**Ответ: б**

**Задание 3**

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
г) нет правильного ответа

**Ответ: в**

**Задание 4**

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
г) нет правильного ответа

**Ответ: б**

**Задание 5**

Какая из приведенных техник является самой важной при выборе конкретных защитных мер:

а) анализ рисков
б) результаты ALE
в) анализ затрат / выгоды
г) нет правильного ответа

**Ответ: в**

**Задание 6**

Что лучше всего описывает цель расчета ALE:

а) количественно оценить уровень безопасности среды
б) оценить потенциальные потери от угрозы в год
в) количественно оценить уровень безопасности среды
г) нет правильного ответа

**Ответ: б**

**Задание 7**

Тактическое планирование:

а) среднесрочное планирование
б) ежедневное планирование
в) долгосрочное планирование
г) нет правильного ответа

**Ответ: а**

**Задание 8**

Эффективная программа безопасности требует сбалансированного применения:

а) контрмер и защитных механизмов

б) процедур безопасности и шифрования
в) технических и нетехнических методов
г) нет правильного ответа

**Ответ: в**

**Задание 9**

Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:

а) уровень доверия, обеспечиваемый механизмом безопасности
б) внедрение управления механизмами безопасности
в) классификацию данных после внедрения механизмов безопасности
г) нет правильного ответа

**Ответ: а**

**Задание 10**

Что из перечисленного не является целью проведения анализа рисков:

а) выявление рисков
б) делегирование полномочий
в) количественная оценка воздействия потенциальных угроз
г) нет правильного ответа

**Ответ: б**

**Задание 11**

Кто является основным ответственным за определение уровня классификации информации?

а) Руководитель среднего звена
б) Высшее руководство
в) Владелец
г) Пользователь

**Ответ: в**

**Задание 12**

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

Варианты ответа:

а) Сотрудники
б) Хакеры
в) Атакующие
г) Контрагенты (лица, работающие по договору)

**Ответ: а**

**Задание 13**

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

**Ответ: в**

**Задание 14**

Что самое главное должно продумать руководство при классификации данных?

а) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным

б) Необходимый уровень доступности, целостности и конфиденциальности

в) Оценить уровень риска и отменить контрмеры

г) Управление доступом, которое должно защищать данные

**Ответ: б**

**Задание 15**

Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

а) Владельцы данных

б) Пользователи

в) Администраторы

г) Руководство

**Ответ: г**

**Задание 16**

Что такое процедура?

а) Правила использования программного и аппаратного обеспечения в компании

б) Пошаговая инструкция по выполнению задачи

в) Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах

г) Обязательные действия

**Ответ: б**

**Задание 17**

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

а) Поддержка высшего руководства

б) Эффективные защитные меры и методы их внедрения

в) Актуальные и адекватные политики и процедуры безопасности

г) Проведение тренингов по безопасности для всех сотрудников

**Ответ: а**

**Задание 18**

Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

а) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски

б) Когда риски не могут быть приняты во внимание по политическим соображениям

в) Когда необходимые защитные меры слишком сложны

г) Когда стоимость контрмер превышает ценность актива и потенциальные потери

**Ответ: г**

**Задание 19**

Что такое политики безопасности?

а) Пошаговые инструкции по выполнению задач безопасности

б) Общие руководящие требования по достижению определенного уровня безопасности

в) Широкие, высокоуровневые заявления руководства

г) Детализированные документы по обработке инцидентов безопасности

**Ответ: в**

**Задание 20**

Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

а) Анализ рисков

б) Анализ затрат / выгоды

в) Результаты ALE

г) Выявление уязвимостей и угроз, являющихся причиной риска

**Ответ: б**