1. **К какой степени секретности относятся сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно- розыскной деятельности, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких из перечисленных**
    a. Совершенно секретные сведения
    b. Секретные сведения
    c. Конфиденциальные

ПК-31.2. К какой степени секретности относятся сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ... (Множественный выбор / Только один ответ)

---

2. **К программным компонентам контроля «Kaspersky Endpoint Security» относятся, выберите правильные**
    a. гарантированное затирание данных
    b. веб контроль
    c. контроль целостности

ПК-31.2. К программным компонентам контроля «Kaspersky Endpoint Security» относятся, выберите правильные (Множественный выбор / Только один ответ)

---

3. **Какая из перечисленных защитных подсистем входит в базовый состав СЗИ НСД «Secret Net»**
    a. Подсистема сетевой защиты
    b. Подсистема контроля целостности
    c. Подсистема защиты от вирусов и вредоносного ПО

ПК-31.2. Какая из перечисленных защитных подсистем входит в базовый состав СЗИ НСД «Secret Net» (Множественный выбор / Только один ответ)

---

4. **Какая из перечисленных защитных подсистем не входит в состав СЗИ НСД Dallas Lock**
    a. Подсистема Замкнутой программной среды для пользователей
    b. Подсистема управления доступом
    c. Подсистема контроля целостности

ПК-31.2. Какая из перечисленных защитных подсистем не входит в состав СЗИ НСД Dallas Lock (Множественный выбор / Только один ответ)

---

5. **Какие механизмы защиты используют методы систем искусственного интеллекта в САВЗ «Kaspersky Endpoint Security»**
    a. Сигнатурный анализ
    b. Эвристический анализ
    c. Контроль устройств

ПК-31.2. Какие механизмы защиты используют методы систем искусственного интеллекта в САВЗ «Kaspersky Endpoint Security» (Множественный выбор / Только один ответ)

---

6. **Межсетевой экран – это**
    a. Локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в АС или выходящей из АС

b. Комплекс организационных мер и программно-технических средств защиты от несанкционированного доступа к информации (несанкционированных действий с ней) в автоматизированной системе
c. Вычислительная сеть, поддерживающая в пределах ограниченной территории один или несколько высокоскоростных каналов передачи цифровой информации

ПК-31.2. Межсетевой экран – это (Множественный выбор / Только один ответ)

---

7. Не является электронным аппаратно-программным идентификатором, выберите правильный ответ

a. IButton, Рутокен, eToken
b. АПМДЗ «Соболь»
c. USB ключи, USB токены

ПК-31.2. Не является электронным аппаратно-программным идентификатором, выберите правильный ответ (Множественный выбор / Только один ответ)

---

8. Недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которые могут быть использованы для реализации угроз безопасности это –

a. Сбой в работе аппаратного и программного обеспечения ИС
b. Уязвимость
c. Ошибка при проектировании и разработке программного (программно-аппаратного) обеспечения ИС

ПК-31.2. Недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которые могут быть использованы для реализации угроз безопасности это – (Множественный выбор / Только один ответ)

---

9. Средства защиты информации от НСД должны использоваться

a. Уязвимость
b. Сбой в работе аппаратного и программного обеспечения ИС
c. Ошибка при проектировании и разработке программного (программно-аппаратного) обеспечения ИС

ПК-31.2. Средства защиты информации от НСД должны использоваться (Множественный выбор / Только один ответ)

---

10. Функция не свойственная аппаратно-программному модулю доверенной загрузки «Соболь»

a. Идентификация и аутентификация пользователей компьютера при их входе в систему с помощью электронных идентификаторов iButton, Рутокен, eToken PRO, eToken PRO (Java), iKey 2032 и др
b. Обеспечение обнаружения и блокирования вторжений основных угроз безопасности на этапе загрузке
c. Контроль целостности программного и аппаратного обеспечения защищаемого компьютера до загрузки ОС - файлов и физических секторов жесткого диска, элементов системного реестра компьютера, журнала транзакций, PCI-устройств, структур SMBIOS, таблиц ACPI, конфигурации оперативной памяти

ПК-31.2. Функция не свойственная аппаратно-программному модулю доверенной загрузки «Соболь» (Множественный выбор / Только один ответ)

Тема 1-2

1. **Аппаратные средства защиты включают в себя**
    a. охрану оборудования и наблюдение за ним
    b. средства защиты серверов
    c. средства защиты памяти

ПК-32.2. Аппаратные средства защиты включают в себя (Множественный выбор / Только один ответ)

---

2. **Защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности – это**
    a. Многоуровневая защита
    b. Модель разграничения доступа
    c. Дискреционная модель

ПК-32.2. Защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности – это (Множественный выбор / Только один ответ)

---

3. **Какая система обеспечивает защиту от модификации критичных файлов ОС, как на этапе загрузки, так и в последующем в процессе ее функционирования?**
    a. Система контроля целостности и аутентичности
    b. Система аутентификации и авторизации
    c. Система межсетевого экранирования

ПК-32.2. Какая система обеспечивает защиту от модификации критичных файлов ОС, как на этапе загрузки, так и в последующем в процессе ее функционирования? (Множественный выбор / Только один ответ)

---

4. **Конфиденциальность данных это**
    a. Способность обеспечивать ее неизменность (физическая целостность) и непротиворечивость (логическая целостность) в процессе хранения и обработки данных
    b. Способность точно и своевременно выполнять все свои функции. Для надежности обработки данных необходимо отсутствие ошибок в программных и аппаратных средствах ВС, что достигается в процессе разработки и сопровождения соответствующих компонентов
    c. Доступность их только для тех лиц, которые имеют на это соответствующие полномочия. При этом необходимо обеспечить защиту не только данных от НС получения, но и защиту программ от несанкционированного распространения

ПК-32.2. Конфиденциальность данных это (Множественный выбор / Только один ответ)

---

5. **По типу ПО уязвимости ПО делятся на?**
    a. Уязвимости системного ПО и ПО пользователя
    b. Уязвимости механизмов аутентификации и прикладного ПО
    c. Уязвимости системного ПО и прикладного ПО

ПК-32.2. По типу ПО уязвимости ПО делятся на? (Множественный выбор / Только один ответ)

---

6. **Порядок использования ресурсов автоматизированной системы, при котором субъекты получают доступ к объектам системы в строгом соответствии с установленными правилами – это**
    a. Идентификация

b. Аутентификация
c. Разграничение доступа

ПК-32.2. Порядок использования ресурсов автоматизированной системы, при котором субъекты получают доступ к объектам системы в строгом соответствии с установленными правилами – это (Множественный выбор / Только один ответ)

---

7. Что обеспечивает дискреционная модель защиты информации?

a. Управление доступом, основанное на правилах секретного документооборота, где документам и участникам назначается уровень безопасности
b. Управление доступом на основе матрицы прав доступа для ролей и правил, регламентирующих назначение ролей пользователям и их активацию во время сеансов
c. Произвольное управление доступом субъектов к объектам и контроль за распространением прав доступа

ПК-32.2. Что обеспечивает дискреционная модель защиты информации? (Множественный выбор / Только один ответ)

---

8. Что относится к основным методам программно-аппаратной защиты?

a. Аппаратные
b. Программные
c. Эталонных характеристик

ПК-32.2. Что относится к основным методам программно-аппаратной защиты? (Множественный выбор / Только один ответ)

---

9. Что относиться к методам защиты информации?

a. Технические
b. Политические
c. Систематические

ПК-32.2. Что относиться к методам защиты информации? (Множественный выбор / Только один ответ)

---

10. Что относиться к парольным методам проверки подлинности пользователя?

a. Методы проверки подлинности на основе комбинированного пароля
b. Методы проверки подлинности на основе сложного пароля
c. Методы проверки подлинности на основе динамически изменяющегося пароля

ПК-32.2. Что относиться к парольным методам проверки подлинности пользователя? (Множественный выбор / Только один ответ)

Тема 1

1. Антропогенные источники информации делятся на

a. Внешние
b. Локальные
c. Внутренние
d. Международные

ПК-32.2. Антропогенные источники информации делятся на (Множественный выбор)

---

2. **ПК-32.2. Верно ли утверждение - Защита ИПО - использование средств и методов, принятие мер и осуществление мероприятий с целью обеспечения безопасности хранимой и обрабатываемой информации, а также используемых в ВС программных средств?**
    a. Нет
    b. Да

ПК-32.2. Верно ли утверждение - Защита ИПО - использование средств и методов,... (Множественный выбор / Только один ответ)

---

3. **Верно ли утверждение - Случайные уязвимости зависят от особенностей окружающей защищаемый объект среды и непредвиденных обстоятельств?**
    a. Да
    b. Нет

ПК-32.2. Верно ли утверждение - Случайные уязвимости зависят от особенностей окружающей защищаемый объект среды и непредвиденных обстоятельств? (Множественный выбор / Только один ответ)

---

4. **Верно ли утверждение - Утечка информации реализуется в виде цепочки или сети условий и факторов и их последствий?**
    a. Да
    b. Нет

ПК-32.2. Верно ли утверждение - Утечка информации реализуется в виде цепочки или сети условий и факторов и их последствий? (Множественный выбор / Только один ответ)

---

5. **Верно ли утверждение - Уязвимость информационной системы представляет собой совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее?**
    a. Да
    b. Нет

ПК-32.2. Верно ли утверждение - Уязвимость информационной системы представляет собой совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или ... (Множественный выбор / Только один ответ)

---

6. **К стихийным источникам угроз относятся**
    a. Представители силовых структур
    b. Различные непредвиденные обстоятельства
    c. Некачественные технические средства обработки информации
    d. Различные решения высших государственных органов, забастовки, войны, революции и т. п.

ПК-32.2. К стихийным источникам угроз относятся (Множественный выбор)

---

7. **Как называется защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации?**
    a. Информационная защита информации
    b. Информационная безопасность
    c. Зашита информации

ПК-32.2. Как называется защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации? (Множественный выбор / Только один ответ)

---

8. Какие есть классы уязвимостей

a. Случайные
b. Субъективные
c. Преднамеренные

ПК-32.2. Какие есть классы уязвимостей (Множественный выбор)

---

9. Какие средства защиты информации регламентируют правила использования, обработки и передачи информации и устанавливают меры ответственности?

a. Законодательные средства
b. Организационные средства
c. Аппаратно-программные

ПК-32.2. Какие средства защиты информации регламентируют правила использования, обработки и передачи информации и устанавливают меры ответственности? (Множественный выбор / Только один ответ)

---

10. Категории информации делятся на

a. Общедоступная
b. Секретная
c. Для служебного пользования
d. С ограниченным доступом

ПК-32.2. Категории информации делятся на (Множественный выбор)

---

11. Конфиденциальность данных - это

a. Способность обеспечивать ее неизменность (физическая целостность) и непротиворечивость (логическая целостность) в процессе хранения и обработки данных
b. Доступность их только для тех лиц, которые имеют на это соответствующие полномочия. При этом необходимо обеспечить защиту не только данных от НС получения, но и защиту программ от несанкционированного распространения
c. Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию

ПК-32.2. Конфиденциальность данных – это (Множественный выбор / Только один ответ)

---

12. На сколько групп делятся источники угроз

a. 5
b. 3
c. 4
d. 7

ПК-32.2. На сколько групп делятся источники угроз (Множественный выбор / Только один ответ)

---

13. Нормативный документ, регламентирующий все аспекты безопасности продукта информационных технологий, называется

a. профилем защиты
b. профилем безопасности
c. стандартом безопасности
d. системой защиты

ПК-32.2. Нормативный документ, регламентирующий все аспекты безопасности продукта информационных технологий, называется (Множественный выбор / Только один ответ)

---

14. Основные объекты информационной безопасности

a. Компьютерные сети, базы данных
b. Информационные системы, психологическое состояние пользователей
c. Бизнес-ориентированные, коммерческие системы

ПК-32.2. Основные объекты информационной безопасности (Множественный выбор / Только один ответ)

---

15. Повреждения делятся на

a. Жизнеобеспечивающие коммуникации
b. Программные закладки
c. Ограждающие конструкции
d. Аппаратные закладки

ПК-32.2. Повреждения делятся на (Множественный выбор)

---

16. Предметная область «ЗИ» подразделяется на

a. процесс ЗИ как совокупность действий по применению методов (способов) и средств ЗИ
b. информационным процессом, протекающим на носителе, или физическим процессом, в котором участвует носитель защищаемой информации
c. обеспечение ЗИ, под которым понимается создание необходимых образовательных, научных, технических, информационных и других условий для реализации процесса ЗИ

ПК-32.2. Предметная область «ЗИ» подразделяется на (Множественный выбор)

---

17. Техногенные источники угроз включают в себя

a. Вспомогательные средства
b. Вспомогательный персонал
c. Наводнения
d. Криминальные структуры

ПК-32.2. Техногенные источники угроз включают в себя (Множественный выбор / Только один ответ)

---

18. Угроза безопасности информации представляет собой

a. Совокупность факторов, создающих реально существующую опасность, связанную с утечкой информации и/или непреднамеренными воздействиями на нее
b. Совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее
c. Совокупность условий и факторов, создающих потенциальную опасность, связанную с утечкой информации или несанкционированными или непреднамеренными воздействиями на нее

ПК-32.2. Угроза безопасности информации представляет собой (Множественный выбор / Только один ответ)

---

19. **Цели защиты ИПО**
    a. ЗИ от хищения
    b. ЗИ от потери
    c. ЗИ от уничтожения

ПК-32.2. Цели защиты ИПО (Множественный выбор)

Тема 2

1. **Аутентификация на основе пароля, переданного по сети в зашифрованном виде, плоха, потому что не обеспечивает защиты от**
    a. Перехвата
    b. Воспроизведения
    c. Атак на доступность

ПК-31.2. Аутентификация на основе пароля, переданного по сети в зашифрованном виде, плоха, потому что не обеспечивает защиты от (Множественный выбор)

---

2. **В АПМДЗ «Соболь» реализованы следующие основные защитные механизмы**
    a. Идентификация и аутентификация пользователей;
    b. Замкнутая программная среда.
    c. Блокировка загрузки ОС со съемных носителей;
    d. Шифрование

ПК-31.2. В АПМДЗ «Соболь» реализованы следующие основные защитные механизмы (Множественный выбор)

---

3. **В качестве аутентификатора в сетевой среде могут использоваться**
    a. Кардиограмма субъекта
    b. Номер карточки пенсионного страхования
    c. Результат работы генератора одноразовых паролей

ПК-31.2. В качестве аутентификатора в сетевой среде могут использоваться (Множественный выбор / Только один ответ)

---

4. **В качестве аутентификатора в сетевой среде могут использоваться**
    a. Год рождения субъекта
    b. Фамилия субъекта
    c. Секретный криптографический ключ

ПК-31.2. В качестве аутентификатора в сетевой среде могут использоваться (Множественный выбор / Только один ответ)

---

5. **В случае ввода пароля, не соответствующего предъявленному идентификатору АПМДЗ «Соболь»**
    a. АПМДЗ «Соболь» оповещает и вызывает администратора по безопасности
    b. Вход пользователя в систему блокируется
    c. Генерируется новый пароль для данного пользователя
    d. Счетчик неудачных попыток входа пользователя в систему увеличивается на единицу

ПК-31.2. В случае ввода пароля, не соответствующего предъявленному идентификатору АПМДЗ «Соболь» (Множественный выбор)

---

6. В случае предъявления персонального идентификатора, не зарегистрированного в системе АПМДЗ «Соболь»

a. Рабочая станция выключается;
b. Вход пользователя в систему блокируется;
c. В журнале регистрации событий фиксируется попытка несанкционированного доступа к компьютеру.
d. Вызывается администратор по безопасности

ПК-31.2. В случае предъявления персонального идентификатора, не зарегистрированного в системе АПМДЗ «Соболь» (Множественный выбор)

---

7. В число основных понятий ролевого управления доступом входит

a. Роль
b. Исполнитель роли
c. Пользователь роли

ПК-31.2. В число основных понятий ролевого управления доступом входит (Множественный выбор / Только один ответ)

---

8. В число основных понятий ролевого управления доступом входит

a. Объект
b. Субъект
c. Метод

ПК-31.2. В число основных понятий ролевого управления доступом входит (Множественный выбор)

---

9. Верно ли утверждение - Под инсталляцией понимается процесс специального копирования или разархивирования программы с дистрибутивных носителей на внешний носитель компьютера и ее настройки под требования пользователя для функционирования на данном компьютере?

a. Да
b. Нет

ПК-31.2. Верно ли утверждение - Под инсталляцией понимается процесс специального копирования или разархивирования программы с дистрибутивных носителей на внешний носитель компьютера и ее настройки под требования пользователя для функционирования на... (Множественный выбор / Только один ответ)

---

10. Виды контроля целостности PCI-устройств

a. Упрощенный
b. Стандартный
c. Адаптивный
d. Регламентированный

ПК-31.2. Виды контроля целостности PCI-устройств (Множественный выбор)

---

11. Выберете правильные парольные методы проверки подлинности пользователей

a. методы проверки подлинности на основе многоразового пароля
b. методы проверки подлинности на основе автоматически созданного пароля
c. методы проверки подлинности на основе одноразового пароля

d. методы проверки подлинности на основе нетривиального пароля

ПК-31.2. Выберете правильные парольные методы проверки подлинности пользователей (Множественный выбор)

---

12. Какие служебные области жесткого диска в комплексе «Соболь» контролируются на целостность

a. Master Boot Record;
b. PCI Express;
c. FAT32

ПК-31.2. Какие служебные области жесткого диска в комплексе «Соболь» контролируются на целостность (Множественный выбор / Только один ответ)

---

13. Какие средства защиты информации связаны применением инструментов шифрования?

a. Организационные средства
b. Аппаратно-программные
c. Криптографические средства

ПК-31.2. Какие средства защиты информации связаны применением инструментов шифрования? (Множественный выбор / Только один ответ)

---

14. Комплекс «Соболь» позволяет контролировать следующие элементы (объекты) системного реестра ОС Windows

a. параметры
b. данные
c. ключи реестра с параметрами и вложенными ключами
d. Версии ПО

ПК-31.2. Комплекс «Соболь» позволяет контролировать следующие элементы (объекты) системного реестра ОС Windows (Множественный выбор)

---

15. Контроль целостности PCI-устройств в АПМДЗ «Соболь» распространяется на следующие шины

a. Mini PCI Express
b. NTFS
c. PCI-X
d. FAT32

ПК-31.2. Контроль целостности PCI-устройств в АПМДЗ «Соболь» распространяется на следующие шины (Множественный выбор)

---

16. Контроль целостности в комплексе «Соболь» направлен на проверку сведений о незавершенных операциях в журнале транзакций

a. Boot Sector;
b. NTFS;
c. FAT32

ПК-31.2. Контроль целостности в комплексе «Соболь» направлен на проверку сведений о незавершенных операциях в журнале транзакций (Множественный выбор)

---

17. Может ли аппаратно-программная среда привязаться к уникальным характеристикам корпуса ЭВМ

a. Да
b. Нет

ПК-31.2. Может ли аппаратно-программная среда привязаться к уникальным характеристикам корпуса ЭВМ (Множественный выбор / Только один ответ)

---

18. Обеспечение защиты СВТ и АС осуществляется

a. системой разграничения доступа (СРД) субъектов к объектам доступа
b. подбором и обучением квалифицированного персонала
c. обеспечивающими средствами для СРД

ПК-31.2. Обеспечение защиты СВТ и АС осуществляется (Множественный выбор)

---

19. Относится ли контроль времени выполнения отдельных частей программы к дополнительному методу защиты от модификаций

a. Нет
b. Да

ПК-31.2. Относится ли контроль времени выполнения отдельных частей программы к дополнительному методу защиты от модификаций (Множественный выбор / Только один ответ)

---

20. Под некорректным действием понимается

a. разрешенное администрацией действие программы или пользователя, которое может привести к нарушению целостности хранящихся данных, а также сбоям или отказам программно-аппаратных средств
b. несанкционированное исследование, копирование или модификация программ

ПК-31.2. Под некорректным действием понимается (Множественный выбор / Только один ответ)

---

21. Под несанкционированным действием пользователя или его программы понимается выполнение любой из следующих запрещенных администрацией операций

a. несанкционированное чтение или копирование данных
b. несанкционированная модификация информации
c. непосредственно сбой или отказ в работе программно-аппаратных средств

ПК-31.2. Под несанкционированным действием пользователя или его программы понимается выполнение любой из следующих запрещенных администрацией операций (Множественный выбор)

---

22. Ролевое управление доступом использует следующее средство объектно-ориентированного подхода

a. Инкапсуляция
b. Наследование
c. Полиморфизм

ПК-31.2. Ролевое управление доступом использует следующее средство объектно-ориентированного подхода (Множественный выбор / Только один ответ)

---

23. Сколько действий содержит алгоритм опознания с использованием простого пароля

a. 4
b. 5
c. 3
d. 7

ПК-31.2. Сколько действий содержит алгоритм опознания с использованием простого пароля (Множественный выбор / Только один ответ)

---

24. Сколько классов защищенности СВТ от НСД к информации

a. 3
b. 7
c. 5

ПК-31.2. Сколько классов защищенности СВТ от НСД к информации (Множественный выбор / Только один ответ)

---

25. Сколько определено уровней контроля на отсутствие не декларированных возможностей

a. 5
b. 3
c. 4

ПК-31.2. Сколько определено уровней контроля на отсутствие не декларированных возможностей (Множественный выбор / Только один ответ)

---

26. Сколько существует методов обнаружения компьютерных вирусов?

a. 4
b. 5
c. 8
d. 14

ПК-31.2. Сколько существует методов обнаружения компьютерных вирусов? (Множественный выбор / Только один ответ)

---

27. Цифровой сертификат содержит

a. Открытый ключ пользователя
b. Секретный ключ пользователя
c. Имя пользователя

ПК-31.2. Цифровой сертификат содержит (Множественный выбор / Только один ответ)

---

28. Аппаратные средства защиты включают в себя

a. противопожарная защита
b. охрана оборудования и наблюдение за ним
c. средства защиты терминалов

ПК-32.2. Аппаратные средства защиты включают в себя (Множественный выбор / Только один ответ)

---

29. **Верно ли утверждение - Идентификация– процедура проверки подлинности, позволяющая достоверно убедиться, что пользователь является именно тем, кем он себя объявляет?**
    a. Нет
    b. Да

ПК-32.2. Верно ли утверждение - Идентификация– процедура проверки подлинности, позволяющая достоверно убедиться, что пользователь является именно тем, кем он себя объявляет? (Множественный выбор / Только один ответ)

---

30. **Верно ли утверждение - Политика безопасности - набор законов, правил и практических рекомендаций, на основе которых строится управление, защита и распределение критичной информации в системе. Она должна охватывать все особенности процесса обработки информации, определяя поведение системы в различных ситуациях. Ее реализация осуществляется при помощи средств управления механизмами защиты?**
    a. Да
    b. Нет

ПК-32.2. Верно ли утверждение - Политика безопасности - набор законов, правил и практических рекомендаций, на основе которых строится управление, защита и распределение критичной информации в системе. Она должна охватывать все особенности процесса ... (Множественный выбор / Только один ответ)

---

31. **Верно ли утверждение - Система защиты информации (СЗИ) - это комплекс организационных мер и программно-технических (в том числе криптографических) средств обеспечения безопасности информации в автоматизированных системах?**
    a. Да
    b. Нет

ПК-32.2. Верно ли утверждение - Система защиты информации (СЗИ) - это комплекс организационных мер и программно-технических (в том числе криптографических) средств обеспечения безопасности информации в автоматизированных системах? (Множественный выбор / Только один ответ)

---

32. **Верно ли утверждение - Цифровой водяной знак (ЦВЗ) – специальная метка, незаметно внедряемая в изображение или другой сигнал с целью контролировать его использование**
    a. Нет
    b. Да

ПК-32.2. Верно ли утверждение - Цифровой водяной знак (ЦВЗ) – специальная метка, незаметно внедряемая в изображение или другой сигнал с целью контролировать его использование (Множественный выбор / Только один ответ)

---

33. **Верно ли утверждение Аутентификация – это процедура распознавания пользователя по его идентификатору (имени)**
    a. Нет
    b. Да

ПК-32.2. Верно ли утверждение Аутентификация – это процедура распознавания пользователя по его идентификатору (имени) (Множественный выбор / Только один ответ)

---

34. **Выберите правильное определение - Криптографические средства защиты информации – это**

a. Регламентируют деятельность людей в сфере информатизации и защиты информации
b. Позволяют решать вопросы обеспечения безопасности информации при наличии физического доступа к объектам защиты потенциальных нарушителей
c. Подразумевают фиксацию факта передачи смены с перечислением того, что и в каком состоянии передается

ПК-32.2. Выберите правильное определение - Криптографические средства защиты информации – это (Множественный выбор / Только один ответ)

---

35. Какие средства защиты информации встроены в блоки информационной системы (сервера, компьютеры и т.д.) и предназначены для внутренней защиты элементов вычислительной техники и средств связи?

a. Аппаратные
b. Программные
c. Физические

ПК-32.2. Какие средства защиты информации встроены в блоки информационной системы (сервера, компьютеры и т.д.) и предназначены для внутренней защиты элементов вычислительной техники и средств связи? (Множественный выбор / Только один ответ)

---

36. Какие существуют парольные методы проверки подлинности пользователя

a. методы проверки подлинности на основе комбинированного пароля
b. методы проверки подлинности на основе сложного пароля
c. методы проверки подлинности на основе простого пароля
d. методы проверки подлинности на основе динамически изменяющегося пароля

ПК-32.2. Какие существуют парольные методы проверки подлинности пользователя (Множественный выбор)

---

37. Какой метод защиты информации связан с регулированием использования всех ресурсов информационной системы?

a. Маскировка
b. Препятствие
c. Управление доступом

ПК-32.2. Какой метод защиты информации связан с регулированием использования всех ресурсов информационной системы? (Множественный выбор / Только один ответ)

---

38. Что входит в методы защиты информации

a. Политические
b. Программно-аппаратные
c. Систематические

ПК-32.2. Что входит в методы защиты информации (Множественный выбор)

---

39. Что относится к основным методам программно-аппаратной защиты

a. Аппаратные
b. Криптографические
c. Комбинированные
d. Эталонных характеристик

ПК-32.2. Что относится к основным методам программно-аппаратной защиты (Множественный выбор)

Тема 3

1. **Агрессивное потребление ресурсов является угрозой**
   a. Доступности
   b. Конфиденциальности
   c. Целостности

ПК-31.2. Агрессивное потребление ресурсов является угрозой (Множественный выбор / Только один ответ)

---

2. **Вирус – это**
   a. Код обладающий способностью к самораспространению путем создания себе подобных копий
   b. Способность объекта реагировать на запрос сообразно своему типу, при этом одно и то же имя метода может использоваться для различных классов объектов
   c. Небольшая программа для выполнения определенной задачи

ПК-31.2. Вирус – это (Множественный выбор / Только один ответ)

---

3. **Вредоносная программа, которая подменяет собой загрузку некоторых программ при загрузке системы называется**
   a. Макровирус
   b. Загрузочный вирус
   c. Троян
   d. Сетевой червь
   e. Файловый вирус

ПК-31.2. Вредоносная программа, которая подменяет собой загрузку некоторых программ при загрузке системы называется (Множественный выбор / Только один ответ)

---

4. **Для внедрения бомб чаще всего используются ошибки типа**
   a. Отсутствие проверок кодов возврата
   b. Переполнение буфера
   c. Нарушение целостности транзакций

ПК-31.2. Для внедрения бомб чаще всего используются ошибки типа (Множественный выбор / Только один ответ)

---

5. **К биометрической системе защиты относятся**
   a. Защита паролем
   b. Идентификация по радужной оболочке глаз
   c. Физическая защита данных
   d. Антивирусная защита
   e. Идентификация по отпечаткам пальцев

ПК-31.2. К биометрической системе защиты относятся (Множественный выбор)

---

6. **К вредоносному программному обеспечению относятся**
   a. Вирусы, черви, трояны
   b. Шпионские и рекламные программы
   c. Вирусы, программы-шутки, антивирусное программное обеспечение
   d. Межсетевой экран, брандмауэр

ПК-31.2. К вредоносному программному обеспечению относятся (Множественный выбор)

7. К основным типам средств воздействия на компьютерную сеть относится

a. Компьютерный сбой
b. Логические закладки («мины»)
c. Аварийное отключение питания

ПК-31.2. К основным типам средств воздействия на компьютерную сеть относится (Множественный выбор / Только один ответ)

---

8. Когда получен спам по e-mail с приложенным файлом, следует

a. Прочитать приложение, если оно не содержит ничего ценного – удалить
b. Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
c. Удалить письмо с приложением, не раскрывая (не читая) его

ПК-31.2. Когда получен спам по e-mail с приложенным файлом, следует (Множественный выбор / Только один ответ)

---

9. Наиболее распространены угрозы информационной безопасности корпоративной системы

a. Покупка нелицензионного ПО
b. Ошибки эксплуатации и неумышленного изменения режима работы системы
c. Сознательного внедрения сетевых вирусов

ПК-31.2. Наиболее распространены угрозы информационной безопасности корпоративной системы (Множественный выбор / Только один ответ)

---

10. Окно опасности появляется, когда

a. Становится известно о средствах использования уязвимости
b. Появляется возможность использовать уязвимость
c. Устанавливается новое ПО

ПК-31.2. Окно опасности появляется, когда (Множественный выбор / Только один ответ)

---

11. По механизму распространения вредоносное ПО различают

a. Вирусы
b. Черви
c. Все ответы правильные

ПК-31.2. По механизму распространения вредоносное ПО различают (Множественный выбор / Только один ответ)

---

12. Политика безопасности

a. Фиксирует правила разграничения доступа
b. Отражает подход организации к защите своих информационных активов
c. Описывает способы защиты руководства организации

ПК-31.2. Политика безопасности (Множественный выбор / Только один ответ)

---

13. Политика информационной безопасности - это

a. Совокупность законов, правил, определяющих управленческие и проектные решения в области защиты информации
b. Стандарт безопасности
c. Профиль защиты
d. Итоговый документ анализа рисков

ПК-31.2. Политика информационной безопасности – это (Множественный выбор / Только один ответ)

---

14. Принцип усиления самого слабого звена можно переформулировать как

a. Принцип равнопрочности обороны
b. Принцип удаления слабого звена
c. Принцип выявления главного звена, ухватившись за которое, можно вытянуть всю цепь

ПК-31.2. Принцип усиления самого слабого звена можно переформулировать как (Множественный выбор / Только один ответ)

---

15. Программа Melissa - это

a. Бомба
b. Вирус
c. Червь

ПК-31.2. Программа Melissa – это (Множественный выбор / Только один ответ)

---

16. Системы анализа защищенности помогают предотвратить

a. Известные атаки
b. Новые виды атак
c. Нетипичное поведение пользователей

ПК-31.2. Системы анализа защищенности помогают предотвратить (Множественный выбор / Только один ответ)

---

17. ПК-31.2. Среди нижеперечисленных отметьте две троянские программы : Среди нижеперечисленных отметьте две троянские программы

a. I LOVE YOU
b. Back Orifice
c. Netbus

ПК-31.2. Среди нижеперечисленных отметьте две троянские программы : Среди ... (Множественный выбор)

---

18. Туннелирование может использоваться на следующем уровне эталонной семиуровневой модели

a. Сетевом
b. Сеансовом
c. Уровне представления

ПК-31.2. Туннелирование может использоваться на следующем уровне эталонной семиуровневой модели (Множественный выбор / Только один ответ)

---

19. Черви – это

a. Вредоносные программы, устанавливающие скрытно от пользователя другие вредоносные программы и утилиты

b. Вирусы, которые проникнув на компьютер, блокируют работу сети
c. Вирусы, которые внедряются в документы под видом макросов
d. Хакерские утилиты управляющие удаленным доступом компьютера
e. Вредоносные программы, которые проникают на компьютер, используя сервисы компьютерных сетей

ПК-31.2. Черви – это (Множественный выбор / Только один ответ)

---

20. ЭЦП – это

a. Электронно-цифровой преобразователь
b. Электронно-цифровая подпись
c. Электронно-цифровой процессор

ПК-31.2. ЭЦП – это (Множественный выбор / Только один ответ)

---

21. Демилитаризованная зона располагается

a. Перед внешним межсетевым экраном
b. Между межсетевыми экранами
c. За внутренним межсетевым экраном

ПК-32.2. Демилитаризованная зона располагается (Множественный выбор / Только один ответ)

---

22. При анализе стоимости защитных мер следует учитывать

a. Расходы на закупку оборудования
b. Расходы на закупку программ и на обучение персонала
c. Оба варианта верны

ПК-32.2. При анализе стоимости защитных мер следует учитывать (Множественный выбор / Только один ответ)

---

23. Среднее время наработки на отказ

a. Пропорционально интенсивности отказов
b. Обратно пропорционально интенсивности отказов
c. Не зависит от интенсивности отказов

ПК-32.2. Среднее время наработки на отказ (Множественный выбор / Только один ответ)

---

24. Экранирование на сетевом и транспортном уровнях может обеспечить

a. Разграничение доступа по сетевым адресам
b. Выборочное выполнение команд прикладного протокола
c. Контроль объема данных, переданных по TCP-соединению

ПК-32.2. Экранирование на сетевом и транспортном уровнях может обеспечить (Множественный выбор / Только один ответ)
