Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Белгородский государственный аграрный университет имени В.Я. Горина»

Кафедра информатики и информационных технологий
(наименование кафедры)

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

ОП.13 Информационная безопасность
(наименование дисциплины)

09.02.05 «Прикладная информатика(по отраслям)»
(код и наименование направления подготовки)

технический
(наименование профиля подготовки)

техник - программист
Квалификация (степень) выпускника

п. Майский, 2020

Паспорт фонда оценочных средств
ОП.13 Информационная безопасность

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1	**Раздел 1.** Информационная безопасность и уровни ее обеспечения	**ПК1.1, ОК1, ОК4, ОК5, ОК6, ОК7, ОК8, ОК9**	Коллоквиум, тест, подготовка реферата
2	**Раздел 2.** Компьютерные вирусы и защита от них.	**ПК 1.2, ОК1, ОК2, ОК3, ОК4, ОК5, ОК6, ОК7, ОК8, ОК9**	Коллоквиум, тест, подготовка реферата, решение кейс-задачи.
3	**Раздел 3.** Информационная безопасность вычислительных сетей.	**ПК1.5, ОК2, ОК3, ОК4, ОК5, ОК6, ОК7, ОК8**	Коллоквиум, тест, подготовка реферата
4	**Раздел 4.** Механизмы обеспечения «информационной безопасности».	**ПК3.3, ОК1, ОК2, ОК3, ОК5, ОК6, ОК7, ОК9**	Коллоквиум, тест, подготовка реферата, решение кейс-задачи.
5	**Зачёт**	**ПК 1.1, ПК 1.2, ПК 1.5, ПК3.3, ОК1 - ОК9**	Вопросы к зачёту

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Белгородский государственный аграрный университет им. В.Я. Горина»

Кафедра Информатики и ИТ

Вопросы для коллоквиумов по разделам

по дисциплине: Информационная безопасность
(наименование дисциплины)

Раздел 1. Информационная безопасность и уровни ее обеспечения

1. Современное состояние информационных технологий. Проблема защиты информации и этапы ее возможного решения.
2. Понятие ИБ. Объекты, цели и задачи ЗИ. Составляющие ИБ.
3. Распространение объектно-ориентированного подхода на ИБ.
4. Техническое обеспечение информационной безопасности.
5. Административный уровень защиты информации: политика безопасности.
   Административный уровень защиты информации: программа безопасности.
   Защита баз данных.
6. Закон об авторском праве.
7. Обзор российского законодательства в области защиты информации.
8. Федеральный закон «Об информации, информационных технологиях и о защите информации».

Раздел 2. Компьютерные вирусы и защита от них.

1. Компьютерный вирус: понятие, пути проникновения.
2. Классификация компьютерных вирусов.
3. Способы заражения программ.
4. Признаки появления вирусов.
5. Защита от воздействия вирусов: понятие антивирусной программы.
6. Классификация антивирусных программ.
7. Способы обнаружения вирусов.
8. Описание распространенных антивирусных программ и комплексов.

Раздел 3. Информационная безопасность вычислительных сетей.

1. Угрозы ИБ: основные понятия. Виды и классификация угроз.
2. Основные угрозы целостности, конфиденциальности, доступности. Примеры.
3. Виды мер обеспечения ИБ.
4. Особенности ЗИ в ПК.
5. Защита информации в сети.
6. Средства защиты кабельной системы.
7. Прокси - серверы.
8. Атака типа отказ в обслуживании.
9. Защита ПК от несанкционированного доступа. Защита от несанкционированной загрузки ОС.

Раздел 4. Механизмы обеспечения «информационной безопасности».

1. Экранирование, фильтрация, заземление, электромагнитное зашумление.
2. Программные средства защиты информации.
3. Разграничение прав пользователей в ОС Windows.
4. Идентификация и аутентификация: понятия, задачи. Аутентификация пользователей на основе паролей.
5. Идентификация и аутентификация: понятия, способы идентификации, Аутентификация пользователей по их биометрическим характеристикам.
6. Протоколирование и аудит: понятие, задачи, примеры.
7. Активный аудит: понятие, задачи, функциональные компоненты.
8. Разграничение доступа: понятие, методы.
9. Криптографические меры защиты информации: основные понятия, методы и алгоритмы шифрования.
10. Шифры перестановки и шифры замены.
11. Симметричные алгоритмы шифрования. Алгоритм DES.
12. Ассиметричные алгоритмы шифрования. Алгоритм RSA.
13. Хэш-функции. Электронная цифровая подпись.
14. Цели интеграции межсетевых экранов.
15. Достоинства аппаратных брандмауэров.

Критерии оценки:

Отметка «5»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, литературным языком. Ответ самостоятельный.

Отметка «4»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки, исправленные по требованию преподавателя.

Отметка «3»: ответ полный, но при этом допущена существенная ошибка, или неполный, несвязный.

Отметка «2»: при ответе обнаружено непонимание обучающимся основного содержания учебного материала или допущены существенные ошибки, которые он не смог исправить при наводящих вопросах преподавателя.

Составитель _____ И.О. Фамилия
(подпись)

«____»_____20 г.

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Белгородский государственный аграрный университет им. В.Я. Горина»

Кафедра Информатики и ИТ

Фонд тестовых заданий

по ОП.13 Информационная безопасность
(наименование дисциплины)

Раздел 1. Информационная безопасность и уровни ее обеспечения

Как называется умышленно искаженная информация?
+ Дезинформация
- Информативный поток
- Достоверная информация
- Перестает быть информацией

Как называется информация, к которой ограничен доступ?
+ Конфиденциальная
- Противозаконная
- Открытая
- Недоступная

Какими путями может быть получена информация?
+ проведением, покупкой и противоправным добыванием информации научных исследований
- захватом и взломом ПК информации научных исследований
- добыванием информации из внешних источников и скремблированием информации научных исследовании
- захватом и взломом защитной системы для информации научных исследований

Основной документ, на основе которого проводится политика информационной безопасности?
+ программа информационной безопасности
- регламент информационной безопасности
- политическая информационная безопасность
- Протекторат

В зависимости от формы представления информация может быть разделена на?
+ Речевую, документированную и телекоммуникационную
- Мысль, слово и речь
- цифровая, звуковая и тайная
- цифровая, звуковая

К каким процессам относят процессы сбора, обработки, накопления,

хранения, поиска и распространения информации
+ Информационным процессам
- Мыслительным процессам
- Машинным процессам
- Микропроцессам

Что называют защитой информации?
+ Все ответы верны
- Называют деятельность по предотвращению утечки защищаемой информации
- Называют деятельность по предотвращению несанкционированных воздействий на защищаемую информацию
- Называют деятельность по предотвращению непреднамеренных воздействий на защищаемую информацию

Под непреднамеренным воздействием на защищаемую информацию понимают?
+ Воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств и воздействие природных явлений
- Процесс ее преобразования, при котором содержание информации изменяется на ложную
- Возможности ее преобразования, при котором содержание информации изменяется на ложную информацию
- Не ограничения доступа в отдельные отрасли экономики или на конкретные производства

Функция защиты информационной системы, гарантирующая то, что доступ к информации, хранящейся в системе может быть осуществлен только тем лицам, которые на это имеют право
- управление доступом
+ конфиденциальность
- аутентичность
- целостность
- доступность

Основные предметные направления Защиты Информации?
+ охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности
- Охрана золотого фонда страны
- Определение ценности информации
- Усовершенствование скорости передачи информации

Государственная тайна это
+ защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны
- ограничения доступа в отдельные отрасли экономики или на конкретные производства
- защищаемые банками и иными кредитными организациями сведения о

банковских операциях
- защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

Меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе

+ Информационная безопасность
- Защитные технологии
- Заземление
- Конфиденциальность

Можно выделить следующие направления мер информационной безопасности

- Правовые
- Организационные
+ Все ответы верны
- Технические

Что можно отнести к правовым мерам ИБ?

+ Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства
- охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра итд
- Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев, установку оборудования обнаружения и тушения пожара, оборудования обнаружения воды, принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое
- охрану вычислительного центра, установку сигнализации и многое другое

Что можно отнести к организационным мерам ИБ?

- Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства.
+ Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.
- Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем.
- Охрану работоспособности отдельных звеньев и организацию вычислительных сетей с возможностью перераспределения ресурсов.
- Принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение

помещений замками, установку сигнализации и многое другое.

Что можно отнести к техническим мерам ИБ?

- Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства
- Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.
+ Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев и многое другое
- Простые и доступные меры защиты от хищений, саботажа, диверсий, взрывов
- В административных местах установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

Обеспечение достоверности и полноты информации и методов ее обработки.

- Конфиденциальность
+ Целостность
- Доступность
- Целесообразность

Обеспечение доступа к информации только авторизованным пользователям?

+ Конфиденциальность
- Целостность
- Доступность
- Целесообразность

Целью информационной безопасности является?

+ все перечисленное
- обезопасить ценности системы
- защитить и гарантировать точность и целостность информации
- минимизировать разрушения

Укажите направления мер информационной безопасности.

+правовые, организационные, технические
-правовые, аппаратные, программные
-личные, организационные
-технические

Что такое Информационная безопасность?

+ меры по защите информации от неавторизованного доступа
-меры по защите ПК
-безопасность личной информации
-все перечисленное

Раздел 2. Компьютерные вирусы и защита от них.

Что такое компьютерный вирус?
Прикладная программа.
Системная программа.
+Программа, выполняющая на компьютере несанкционированные действия.
База данных.
Основные типы компьютерных вирусов:
Аппаратные, программные, загрузочные.
Программные, загрузочные, макровирусы.
+ Файловые, программные, макровирусы.
Этапы действия программного вируса:
Размножение, вирусная атака.
Запись в файл, размножение.
+ Запись в файл, размножение, уничтожение программы.
В чем заключается размножение программного вируса?
Программа-вирус один раз копируется в теле другой программы.
+ Вирусный код неоднократно копируется в теле другой программы.
Что называется вирусной атакой?
Неоднократное копирование кода вируса в код программы.
Отключение компьютера в результате попадания вируса.
+ Нарушение работы программы, уничтожение данных, форматирование жесткого диска.
Какие существуют методы реализации антивирусной защиты?
Аппаратные и программные.
+ Программные и административные.
Только программные.
Какие существуют основные средства защиты данных?
+ Резервное копирование наиболее ценных данных.
Аппаратные средства.
Программные средства.
Какие существуют вспомогательные средства защиты?
Аппаратные средства.
Программные средства.
+ Административные методы и антивирусные программы.
На чем основано действие антивирусной программы?
На ожидании начала вирусной атаки.
+ На сравнении программных кодов с известными вирусами.
На удалении зараженных файлов.
О каком вирусе идет речь?
«Могут привести к сбою и зависанию при работе компьютера»
Файловый
+ Опасный
Загрузочный
Этапы действия программного вируса:
Размножение, вирусная атака.

+ Запись в файл, размножение, уничтожение.
Запись в файл, размножение.
Какие программы относятся к антивирусным?
+ AVP, DrWeb, Norton AntiVirus.
MS-DOS, MS Word, AVP .
MS Word, MS Excel, Norton Commander .
Какие существуют вспомогательные средства защиты?
+ Административные методы и антивирусные программы.
Аппаратные средства.
Программные средства.
В чем заключается размножение программного вируса?
Программа-вирус один раз копируется в теле другой программы.
+ Вирусный код неоднократно копируется в теле другой программы.
Ответьте на вопрос «Что называется вирусной атакой?»
Нарушение работы программы, уничтожение данных, форматирование жесткого диска.
Ответьте на вопрос «Какие существуют методы реализации антивирусной защиты?»
Программные и административные
На чем основано действие антивирусной программы?
На ожидании начала вирусной атаки
+ На сравнении программных кодов с известными вирусами
На удалении зараженных файлов
Какие существуют основные средства защиты данных?
Аппаратные средства
Программные средства
+Резервное копирование наиболее ценных данных

Раздел 3. Информационная безопасность вычислительных сетей.

Меры по защите информации от неавторизованного доступа называется
+Информационной безопасностью
-Безопасностью ПК
-Личной безопасностью
- Безопасностью группы администратора
Средства аппаратной защиты, включающие средства защиты кабельной системы, систем электропитания относится к?
+техническим мерам защиты
- не правовым мерам защиты
-организационным мерам защиты
-программным средствам защиты
Защита от сбоев серверов, рабочих станций и локальных компьютеров относится к?
+аппаратным средствам защиты
-программным средствам защиты

-техническим средствам защиты
-правовым средствам защиты
Защищаемые программы для ПК находятся в?
+ ОЗУ и ЖМД
- ПЗУ и МГД
- МГД и Оп
- ПК и НГМД
К правовым мерам следует отнести?
+ разработку норм, устанавливающих ответственность за компьютерные преступления и защиту авторских прав программистов
-охрану вычислительного центра и аппаратуры связи
- проектирование ЛВС и ГБС
- средства идентификации и аутентификации пользователей
Потеря или изменение данных при ошибках ПО относится к
+ техническим и правовым мерам защиты
-организационным мерам защиты
- правовым мерам защиты
- мерам защиты от НДС и кражи
- к средствам идентификации и аутентификации
Защита от сбоев серверов, рабочих станций и локальных компьютеров относится к?
+Аппаратным и техническим средствам защиты
-Программным средствам защиты
-Средствам защиты идентификации и аутентификации
- Организационным и общим средствам защиты
Какой способ защиты информации присваивает значение каждому пользователю соответствующие права доступа к каждому ресурсу
+Права группы
-Аудит
-Шифрование данных
-Модели защиты
Методы сохранение данных при чрезвычайных ситуаций
-резервное копирование на магнитную ленту;
-источники бесперебойного питания (UPS);
-отказоустойчивые системы
+Все ответы верны
Какой способ данные, дублируя и размещая их на различных физических носителях (например, на разных дисках).
-Журнал резервного копирования
+Отказоустойчивые системы
-Метод резервного копирования
-Шифрование данных
Наиболее надежным средством предотвращения потерь информации при кратковременном отключении электроэнергии?
+ установка источников бесперебойного питания (UPS)

- Такого средства не существует
- Каждую минуту сохранять данные
- Перекидывать информацию на носитель, который не зависит от энергии

Средства защиты данных, функционирующие в составе программного обеспечения.

+ Программные средства защиты информации
- Технические средства защиты информации
- Источники бесперебойного питания (UPS)
- Смешанные средства защиты информации

Средством предотвращения потерь информации при кратковременном отключении электроэнергии является?

+источник бесперебойного питания (UPS)
-источник питания
-электро-переключатель
-все перечисленное

Технические меры защиты можно разделить на:

+ средства аппаратной защиты, включающие средства защиты кабельной системы, систем электропитания, и тд
-правовые, организационные, технические
-правовые, аппаратные, программные
-личные, организационные

Программные средства защиты можно разделить на:

+криптография, антивирусные программы, системы разграничения полномочий, средства контроля доступа и тд
- административные меры защиты, включающие подготовку и обучение персонала, организацию тестирования и приема в эксплуатацию программ, контроль доступа в помещения и тд
-правовые, организационные, технические
-правовые, аппаратные, программные

К наиболее важному элементу аппаратной защиты можно отнести?

+ защита от сбоев серверов, рабочих станций и локальных компьютеров
-защиту от вирусов
-защиту от хакеров
-все перечисленное

Наибольшую угрозу для безопасности сети представляют.

+несанкционированный доступ, электронное подслушивание и преднамеренное или неумышленное повреждение
- вскрытие стандартной учётной записи пользователя
- вскрытие стандартной учётной группы администратора
- копирование файлов, которые были изменены в течение дня, без отметки о резервном копировании

Защита через права доступа заключается.

+присвоении каждому пользователю определенного набора прав
-запереть серверы в специальном помещении с ограниченным доступом
-присвоить пароль каждому общедоступному ресурсу

- в наличии преобразователя микрофона

Дифференцированное резервное копирование это

-Копирование только тех файлов, которые были изменены в течение дня, без отметки о резервном копировании

-Копирование всех выбранных файлов без отметки о резервном копировании

-Копирование и маркировка выбранных файлов, только если они были изменены со времени последнего копирования

+Копирование выбранных файлов, только если они были изменены со времени последнего резервного копирования, без отметки о резервном копировании

Disk mirroring – это

+дублирование раздела и запись его копии на другом физическом диске

-это пара зеркальных дисков, каждым из которых управляет отдельный контроллер

-При записи данных делится на части и распределяется по серверу

- Копирование только тех файлов, которые были изменены в течение дня, без отметки о резервном копировании

Как называются компьютерные системы, в которых обеспечивается безопасность информации?

+ защищенные КС

- небезопасные КС

- Само достаточные КС

- Саморегулирующиеся КС

Элемент аппаратной защиты, где используется резервирование особо важных компьютерных подсистем

- защита от сбоев в электропитании

+ защита от сбоев серверов, рабочих станций и локальных компьютеров

- защита от сбоев устройств для хранения информации

- защита от утечек информации электромагнитных излучений

Элемент аппаратной защиты, где используется организация надежной и эффективной системы резервного копирования и дублирования данных

- защита от сбоев в электропитании

- защита от сбоев серверов, рабочих станций и локальных компьютеров

+ защита от сбоев устройств для хранения информации

- защита от утечек информации электромагнитных излучений

Элемент аппаратной защиты, где используется экранирование, фильтрацию, заземление, электромагнитное зашумление, а также средства ослабления уровней нежелательных электромагнитных излучений.

- защита от сбоев в электропитании

- защита от сбоев серверов, рабочих станций и локальных компьютеров

- защита от сбоев устройств для хранения информации

+ защита от утечек информации электромагнитных излучений

Какая из перечисленных атак на поток информации является пассивной:

+ перехват.
- имитация.
- модификация.
- фальсификация.
- прерывание.

Технические каналы утечки информации делятся на…

+ Все перечисленное
- Акустические и виброакустические
- Электрические
- Оптические

Какой технический канал утечки отвечает за распространение звуковых колебаний в любом звукопроводящем материале или среде?

+ Акустические и виброакустические
- Электрические
- Оптические
- Радиоканалы

Какой технический канал утечки отвечает за напряжение и токи в различных токопроводящих коммуникациях?

- Акустические и виброакустические
+ Электрические
- Оптические
- Радиоканалы

Какой технический канал утечки отвечает за электромагнитные излучения радиодиапазона?

- Акустические и виброакустические
- Электрические
- Оптические
+ Радиоканалы

Какой технический канал утечки отвечает за электромагнитные излучения в видимой, инфракрасной и ультрафиолетовой частях спектра?

- Акустические и виброакустические
- Электрические
+ Оптические
- Радиоканалы

Учет всех возможных коммуникационных каналов, обеспечения физической безопасности, шифрования резервных копий и информации, покидающей корпоративный периметр, и других организационных мероприятий это?

- Индивидуальный подход к защите
+ Комплексный подход к защите
- Смешанный подход к защите
- Рациональный подход к защите информация удаляется

Потенциальные угрозы, против которых направлены технические меры защиты информации

+ Потери информации из-за сбоев оборудования, некорректной работы программ и ошибки обслуживающего персонала и пользователей
- Потери информации из-за халатности обслуживающего персонала и не ведения системы наблюдения
- Потери информации из-за не достаточной установки резервных систем электропитании и оснащение помещений замками.
- Потери информации из-за не достаточной установки сигнализации в помещении.
- Процессы преобразования, при котором

Раздел 4. Механизмы обеспечения «информационной безопасности».

Криптографические средства относится к?
+Программным средствам
-Аппаратным средствам
-Организационным средствам защиты
-Захвату данных
Шифрование информации это
+ Процесс ее преобразования, при котором содержание информации становится непонятным для не обладающих соответствующими полномочиями субъектов
- Процесс преобразования, при котором информация удаляется
- Процесс ее преобразования, при котором содержание информации изменяется на ложную
- Процесс преобразования информации в машинный код
Программные средства защиты информации.
+ средства архивации данных, антивирусные программы
- Технические средства защиты информации
- Источники бесперебойного питания (UPS)
- Смешанные средства защиты информации
Программное средство защиты информации.
+ криптография
- источник бесперебойного питания
- резервное копирование
- дублирование данных
Запуск утилиты Setup выполняется нажатием кнопки?
+Delete
-Alt
-Tab
-F2
Чтобы установить парольную защиту в ОС Windows , необходимо выполнить следующую процедуру?
+Пуск->Панель управления->Учетные записи->Изменение пароля
-Пуск->Учетные записи->Изменение пароля
-Пуск->Справка->Учетные записи->Изменение пароля

-Пуск->Панель управления->Пароли и данные->Изменение пароля
При вводе пароля с клавиатуры его длина может достигать до?
+64 символов
-128 символов
-32 символов
-512 символов
Служат обеспечению сохранения целостности программного обеспечения в составе вычислительной системы
+пароль
-корпус вычислительной системы
-шифры
-сигналы
В каких случаях криптография неэффективна?
+ когда элементы текста известны в зашифрованном и исходном виде
- когда элементы текста известны в открытом и активном виде
- если есть пароль и логин
- когда элементы текста представлены в открытом и не полном виде
В каком случае надежнее шифр?
+короткий зашифрованный текст
-длинный зашифрованный текст
-зашифрованный текст среднего размера
-зашифрованный текст не влияет на надежность шифра
Как связаны ключи шифрования между собой?
+математической функцией
-связкой
-шифром
-специальным паролем
В каких случаях возможно вычисление одного ключа с помощью другого
+ Использованием только ЭВМ
- Ни в каких случаях невозможна
- Использованием математической функцией
- Использованием только ЛВС
Назначение пароля в ИС?
+ механизм управления доступом, средство защиты и безопасность личной информации
- скрытие копирования участков магнитной ленты из ОЗУ в ПЗУ
- технические меры защиты и средство защиты данных
- участки магнитной ленты скрытые шифром
- механизм управления средствами защиты и безопасность доступа к ОЗУ в ПЗУ
Меры по защите информации от неавторизованного доступа называется
+Информационной безопасностью
-Безопасностью ПК
-Личной безопасностью

-Средства защиты
-Меры скрытия копирования

Средства аппаратной защиты, включающие средства защиты кабельной системы, систем электропитания относится к?

+ техническим мерам защиты и правовым мерам защиты
-организационным мерам защиты
- меры скрытия копирования участков магнитной ленты из ОЗУ в ПЗУ

Защита от сбоев серверов, рабочих станций и локальных компьютеров относится к?

+аппаратным средствам защиты
-программным средствам защиты
-техническим средствам защиты
-правовым средствам защиты

Самый известный в России производитель систем защиты от вирусов, спама и хакерских атак.

+лаборатория Касперского
-Российский центр по защите от вредоносных программ
-компания McAfee Security
-лаборатория доктора Веб
-компания Тумар

Один из механизмов защиты использующих в сети для обеспечения конфиденциальности

+управление маршрутизацией
-генерация трафика
-защитный канал
-защитный механизм
-генерация данных

Развитие современных средств безбумажного документооборота, средств электронных платежей немыслимо без развития средств доказательства подлинности и целостности документа. Таким средством является

+ электронно-цифровая подпись
-протокол секретности
-аутентификация
-биометрия
-идентификация пользователя
-водяные знаки

При генерации электронно – цифровой подписи используются…

+общие параметры, секретный ключ и открытый ключ
-открытый ключ, закрытый ключ
-общие параметры, секретный ключ и закрытый ключ
-общие параметры, секретный ключ и конверт защиты
-один секретный ключ

Информация основной объект защиты, ее сохранность и конфиденциальность это основа

+информационной безопасности

-информационной защищенности
-объективность защищенности
-информатики и компьютерных сетей

При каком случае срабатывает сигнал самоуничтожения программы

+при несанкционированном копировании программы из ПЗУ в ОЗУ
-при несанкционированном копировании программы из ОЗУ в ПЗУ
- при непредвиденном включении преобразователя микрофона
-при непредвиденном отключении ПК

Что такое пароль?

+механизм управления доступом
-средство защиты
-безопасность личной информации
- Безопасность людей

Как связаны ключи шифрования между собой?

+математической функцией
-связкой
-шифром
-специальным паролем

Наиболее распространенный криптографический код

+Код Хэмминга
-код Рида-Соломона
-код Морзе
-итеративный код

Критерии оценки:

90-100 баллов «отлично» заслуживает студент, показавший всестороннее систематическое и глубокое знание учебно-программного материала, умение свободно выполнять задания, предусмотренные программой, усвоивший основную и знакомый с дополнительной литературой, рекомендованной программой; как правило, оценка «отлично» выставляется студентам, усвоившим взаимосвязь основных понятий междисциплинарного курса и их значение для приобретаемой профессии, проявившим творческие способности в понимании, изложении и использовании учебно-программного материала;

80-90 баллов «хорошо» заслуживает студент, обнаруживший полное знание учебно-программного материала, успешно выполняющий предусмотренные в программе задания, усвоивший основную литературу, рекомендованную в программе; как правило, оценка «хорошо» выставляется студентам, показавшим систематический характер знаний по дисциплине и способным к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности;

60-80 баллов «удовлетворительно» заслуживает студент, обнаруживший знания основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, справляющийся с выполнением заданий, предусмотренных программой,

знакомый с основной литературой, рекомендованной программой; как правило, оценка «удовлетворительно» выставляется студентам, допустившим погрешности в ответе на зачете, но обладающим необходимыми знаниями для их устранения под руководством преподавателя;

Менее 60 баллов «неудовлетворительно» выставляется студенту, обнаружившему проблемы в знаниях основного учебно-программного материала, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий; как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжать обучение или приступить к профессиональной деятельности по окончании учебного заведения без дополнительных занятий по соответствующему междисциплинарному курсу.

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Белгородский государственный аграрный университет им. В.Я. Горина»

Кафедра Информатики и ИТ

Темы рефератов

по дисциплине Информационная безопасность
(наименование дисциплины)

Раздел 1. Информационная безопасность и уровни ее обеспечения

1. Уровни обеспечения информационной безопасности.
2. Ответственность за нарушения в сфере информационной безопасности.
3. Стандарты информационной безопасности в РФ.
4. Классификация угроз информационной безопасности.

Раздел 2. Компьютерные вирусы и защита от них.

1. Характеристика путей проникновения вирусов в компьютеры.
2. Методы борьбы с распространением «вирусоподобных» программ.
3. Факторы, определяющие качество антивирусных программ.
4. Общий алгоритм обнаружения вируса.

Раздел 3. Информационная безопасность вычислительных сетей.

1. Модель взаимодействия открытых систем OSI/ISO.
2. Адресация в глобальных сетях.
3. Профилактика удаленных угроз в вычислительных сетях.
4. Защита от удаленных угроз в вычислительных сетях.

Раздел 4. Механизмы обеспечения «информационной безопасности».

1. Идентификация пользователя по голосу.
2. Шифрование сообщений.
3. Средства контроля за разграничением прав доступа.
4. Технология виртуальных частных сетей (VPN).

Критерии оценки:

Отметка «5»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, литературным языком. Ответ самостоятельный.

Отметка «4»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, при этом

допущены две-три несущественные ошибки, исправленные по требованию преподавателя.

Отметка «3»: ответ полный, но при этом допущена существенная ошибка, или неполный, несвязный.

Отметка «2»: при ответе обнаружено непонимание обучающимся основного содержания учебного материала или допущены существенные ошибки, которые он не смог исправить при наводящих вопросах преподавателя.

Составитель _____ И.О. Фамилия
(подпись)

«____»_____20 г.

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Белгородский государственный аграрный университет им. В.Я. Горина»

Кафедра Информатики и ИТ

Кейс-задачи

по ОП.13 Информационная безопасность

Раздел 2. Компьютерные вирусы и защита от них.

1. **Описание ситуации**

В ноябре 1988 г. случилась первая эпидемия, вызванная сетевым червем. На офисных компьютерах стояла операционная система Unix. Доступ в интернет имел один компьютер, остальные были связаны с ним по локальной сети. Это позволяло маскироваться под задачу легальных пользователей системы. Однако из-за ошибок в коде безвредная по замыслу программа неограниченно рассылала свои копии по другим компьютерам сети, запускала их на выполнение и таким образом забирала под себя все сетевые ресурсы. Червь Морриса заразил по разным оценкам от 6000 до 9000 компьютеров в США (включая Исследовательский центр NASA) и практически парализовал их работу сроком до пяти суток. Общие убытки были оценены в минимум 8 миллионов часов потери доступа и свыше миллиона часов прямых потерь на возобновление работоспособности систем. Общая стоимость этих расходов оценивается в 96 миллионов долларов.

Вопрос кейса: Представьте себя работниками Исследовательского центра NASA. Предложите варианты выявления заражения, проверки, профилактики, защиты данных.

2. Студент факультета информатики был удивлен, заметив, что во время прослушивания определенного аудиофайла, активируется запуск браузера Internet Explorer, который переходит на страницу Интернета, где пользователю предлагается скачать и установить некий файл, выдаваемый за кодек со странным названием, расширением. Студент несколько раз отвергал установку. Студент описал происходящее на форуме сайта Virusov.net.

Что узнал студент? Какой это вирус? Что он делает? Чем опасен, к чему приводит?

Раздел 4. Механизмы обеспечения «информационной безопасности».

1. Дано исходное сообщение «ЭВМ».

Какое сообщение получится в результате выполнения алгоритма?

Если алгоритм шифрования заключается в следующем

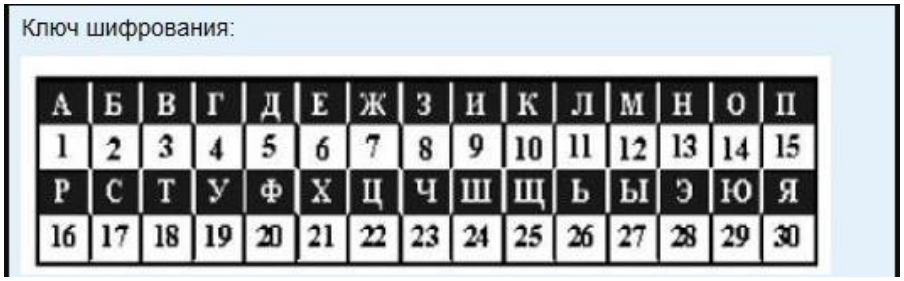
Шаг 1: Найти порядковый номер первой буквы исходного сообщения по ключу.

Шаг 2: К порядковому номеру первой буквы исходного сообщения прибавить цифру 2.

Шаг 3: Полученное число является порядковым номером буквы в зашифрованном сообщении.

Шаг 4: Используя шаги 1-3, зашифровать все буквы исходного сообщения.

Ключ шифрования:



Критерии оценки:

отметка «5»: Задание выполнено в полном объёме с соблюдением необходимой последовательности. Студент работал полностью самостоятельно.

отметка «4»:Практическое задание выполнено студентом в полном объёме и самостоятельно. Допускается отклонение от необходимой последовательности выполнения, не влияющее на правильность конечного результата. Допускаются неточности и небрежность в оформлении результатов задания.

отметка «3»:Практическое задание выполнено и оформлено студентом с помощью преподавателя или хорошо подготовленных и уже выполнивших на «отлично» данную работу студентов. На выполнение задания затрачено много времени.

Отметка «2»:Выставляется в том случае, когда студент оказался неподготовленным к выполнению задания. Полученные результаты не позволяют сделать правильных выводов и полностью расходятся с поставленной целью. Обнаружено плохое знание теоретического материала и отсутствие необходимых умений. Руководство и помощь со стороны преподавателя неэффективны из-за плохой подготовки студента.

Составитель _____ И.О. Фамилия
(подпись)

«___»_____20 г.

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Белгородский государственный аграрный университет им. В.Я. Горина»

Кафедра Информатики и ИТ

Вопросы к зачёту

по дисциплине Информационная безопасность

1. Понятие информационной безопасности. Вопросы информационной безопасности в системе обеспечения национальной безопасности.
2. Основные составляющие и аспекты информационной безопасности.
3. Классификация угроз информационной безопасности: для личности, для общества, для государства.
4. Понятие информационной войны. Особенности информационной войны. Понятие информационного превосходства.
5. Концепция «информационной войны» по оценкам российских спецслужб.
6. Понятие информационного оружия. Что отличает информационное оружие от обычных средств поражения?
7. Сфера применения информационного оружия.
8. Особенности информационного оружия. Организация защиты.
9. Основные задачи в сфере обеспечения информационной безопасности.
10. Отечественные стандарты в области информационной безопасности
11. Зарубежные стандарты в области информационной безопасности
12. Понятие защиты информации. Какая система считается безопасной? Какая система считается надёжной?
13. Основные критерии оценки надежности: политика безопасности и гарантированность.
14. Понятие государственной тайны. Понятие профессиональной тайны.
15. Понятие коммерческой тайны. Понятие служебной тайны. Понятие банковской тайны.
16. Основные конституционные гарантии по охране и защите прав и свобод в информационной сфере.
17. Понятие надежности информации в автоматизированных системах обработки данных. Что понимается под системной защитой информации.
18. Уязвимость информации в автоматизированных системах обработки данных.
19. Элементы и объекты защиты в автоматизированных системах обработки данных.
20. Методы защиты информации от преднамеренного доступа.
21. Защита информации от исследования и копирования.

22. Опознавание с использованием простого пароля. Метод обратимого шифрования.
23. Использование динамически изменяющегося пароля. Методы модификации схемы простых паролей.
24. Использование динамически изменяющегося пароля. Метод «запрос-ответ»
25. Использование динамически изменяющегося пароля. Функциональные методы
26. Криптографические методы защиты информации в автоматизированных системах. Основные направления использования криптографических методов. Симметричные криптосистемы. Системы с открытым ключом.
27. Электронная (цифровая) подпись. Цели применения электронной подписи.
28. Понятие криптостойкости шифра. Требования к криптографическим системам защиты информации.
29. Классификация методов криптографического закрытия.
30. Особенности защиты информации в персональных ЭВМ. Основные цели защиты информации.
31. Угрозы информации в персональных ЭВМ.
32. Обеспечение целостности информации в ПК. Физическая зашита ПК и носителей информации.
33. Защита ПК от несанкционированного доступа.
34. Способы опознавания (аутентификации) пользователей и используемых компонентов обработки информации. Дать краткую характеристику.
35. Классификация закладок. Причины защиты ПК от закладок. Аппаратные закладки.
36. Программные закладки. Классификация критериев вредоносного воздействия закладок.
37. Общие характеристики закладок.
38. Методы и средства защиты от закладок.
39. Компьютерный вирус. Какая программа считается зараженной.
40. По каким признакам классифицируются вирусы?
41. Способы заражения программ. Стандартные методы заражения.
42. Как работает вирус?
43. Методы защиты от вирусов.
44. Антивирусные программы. Программы-детекторы. Программы-доктора.
45. Антивирусы-полифаги. Эвристические анализаторы.
46. Программы-ревизоры. Программы-фильтры.
47. Цели, функции и задачи защиты информации в сетях ЭВМ. Угрозы безопасности для сетей передачи данных.
48. В чём заключаются задачи защиты в сетях передачи данных?
49. Проблемы защиты информации в вычислительных сетях.
50. Понятие сервисов безопасности: идентификация / аутентификация, разграничение доступа.

51. Понятие сервисов безопасности: шифрование, контроль целостности, контроль защищённости, обнаружение отказов и оперативное восстановление.
52. Архитектура механизмов защиты информации в сетях ЭВМ.

Критерии оценки:

- «зачтено» - обучающийся имеет устойчивые знания об основных понятиях дисциплины, может сформулировать взаимосвязи между понятиями;
- «не зачтено» - обучающийся имеет значительные пробелы в знаниях, не может сформулировать взаимосвязи между изучаемыми в курсе понятиями, не имеет представления о большинстве изучаемых основных понятий дисциплины.

Составитель _____ И.О. Фамилия
(подпись)

«____»_____20 г.