МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГАОУ ВО «Тюменский государственный университет»
Тобольский педагогический институт им. Д.И.Менделеева (филиал)
Тюменского государственного университета

УТВЕРЖДАЮ
Заместитель директора филиала
_____ Шитиков П.М.
«03» 02 2023 год

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
ОП.14 МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ
для обучающихся по программе подготовки специалистов среднего звена
09.02.07 Информационные системы и программирование
форма обучения очная

Оленькова Маргарита Николаевна. ОП.14 Методы и средства защиты компьютерной информации. Фонд оценочных средств дисциплины для обучающихся по программе подготовки специалистов среднего звена 09.02.07 Информационные системы и программирование. Форма обучения – очная. Тобольск, 2023.

Фонд оценочных средств дисциплины разработан на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности09.02.07 Информационные системы и программирование, утвержденного приказом Министерства образования и науки Российской Федерации от 9декабря 2016 г. № 1547.

Фонд оценочных средств дисциплины опубликован на сайте ТюмГУ [электронный ресурс] / Режим доступа: https://www.utmn.ru/sveden/education/#

Содержание

1. Общая характеристика фондов оценочных средств

1.1. Область применения программы

Фонд оценочных средств учебной дисциплины «Методы и средства защиты компьютерной информации» является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности 09.02.07 Информационные системы и программирование.

1.2. Место дисциплины в структуре программы подготовки специалистов среднего звена

Дисциплина входит в Общепрофессиональный цикл учебного плана специальности.

1.3. Цели и задачи дисциплины – требования к результатам освоения дисциплины

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОК 01 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности

ОК 04 Эффективно взаимодействовать и работать в коллективе и команде.

ОК 06 Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения.

ПК 11.1 Осуществлять сбор, обработку и анализ информации для проектирования баз данных.

ПК 11.2 Проектировать базу данных на основе анализа предметной области.

ПК 11.6 Защищать информацию в базе данных с использованием технологии защиты информации.

Код ПК, ОК	**Умения**	**Знания**
ОК 01, ОК 02, ОК 04, ОК 06, ПК 11.1, ПК 11.2, ПК 11.6	- применять правовые, организационные, технические и программные средства защиты информации; - проводить оценку угроз безопасности объекта информатизации; - реализовывать простые информационные технологии реализующие методы защиты информации.	- применять правовые, организационные, технические и программные средства защиты информации; - проводить оценку угроз безопасности объекта информатизации; - реализовывать простые информационные технологии реализующие методы защиты информации.

2.Паспорт фонда оценочных средств

п/п	**Темы дисциплины, МДК, разделы (этапы) практики, в ходе текущего контроля, вид промежуточной аттестации с указанием семестра**	**Код контролируемой компетенции (или её части), знаний, умений**	**Наименование оценочного средства (с указанием количество вариантов, заданий и т.п.)**
1.	Раздел 1. Информационная безопасность и уровни ее обеспечения.	ОК 01,ПК11.1	Индивидуальные задания (4 задания), устный опрос(11 вопросов)
2.	Раздел2. Компьютерные вирусы и их защита.	ОК 02, ПК 11.2	Индивидуальные задания (2задания), Контрольные вопросы (7 вопросов)
3.	Раздел3. Информационная безопасность вычислительных сетей.	ОК 04,ПК11.6	Индивидуальные задания (2 задания), устный опрос(12 вопросов)
4.	Раздел4.Механизмы обеспечения «Информационной безопасности».	ОК 06, ПК11.6	Индивидуальные задания (4 задания), устный опрос (19 вопросов)
5.	Промежуточная аттестация в виде комплексного дифференцированного зачета во 2 семестре	ОК 01, ОК 02, ОК 04, ОК 06, ПК 11.1, ПК 11.2, ПК 11.6	Вопросы к дифференцированному зачету (28 вопросов), итоговый тест (28вопросов)

3. Типовые задания для оценки освоения дисциплины

Раздел 1. Информационная безопасность и уровни ее обеспечения.	ОК 01, ПК 11.1

Индивидуальное задание по теме «Средства безопасности ОС Windows»

Цель:

- познакомиться с особенностями шифрования информации в ОС;
- познакомиться с понятием сертификата ОС Windows;
- научиться шифровать и расшифровыть данные;
- научиться работать с сертификатами ОС.

Задания:

1. Создайте на диске С:\Темп папку и скопируйте в нее любой файл.
2. Зашифруйте файл вместе с папкой таким образом, чтобы все помещаемые в папку файлы тоже шифровались (если шифрование не удалось дальнейшие действия с папкой делайте как с зашифрованной).
3. Создайте на рабочем столе папку с вашей фамилией и добавьте в неё резервную копию зашифрованной вами папки (сохраняя шифрование).
4. Установите оснастку Сертификаты.
5. Создайте резервную копию вашего сертификата и поместите ее в вашу папку на рабочем столе.

Контрольные вопросы:

1. Назначение шифрования информации.
2. Какие атрибуты шифрования папки можно указать?
3. Почему необходимо чтобы при копировании или перемещении шифрованной папки пункт назначения поддерживал это шифрование?
4. Как восстановить сертификат из резервной копии?
6. Особенности технология EFS?
7. Что подразумевается под политикой восстановления?

Индивидуальное заданиепо теме «Обеспечения безопасности хранения данных в ОС Windows»

Цель:

- изучить технологию теневого копирования данных и возможность создания отказоустойчивых томов для хранения данных;
- научиться архивировать данные с возможность разграничения доступа к архивам.

Задание 1. Выполните полную, а затем добавочную архивацию с помощью программы Backup. Создайте задания для программы архивации, которые будут выполняться по расписанию.

1. В папке С:\Темп:\Документы создайте три текстовых документа с произвольным содержимым, например, Отчет . txt, Планы.txt и Заказы.txt.
2. В проводнике Windows выберите режим просмотра содержимого папки D:\ Документы в виде таблицы (Меню «Вид» / «Таблица»). Обратите внимание, что в столбце «Атрибуты» у всех трех файлов установлен атрибут «архивный» (бит архива обозначается буквой «А»).
2. Выберите «Пуск» / «Программы» / «Стандартные» / «Служебные» / «Архивация данных». Программа Backup Windows первый раз запускается в режиме мастера. На первой странице мастера (см. рис. 4.5) снимите флажок «Всегда запускать в режиме мастера» и нажмите на ссылку «Расширенный режим». Запустится программа архивации. Перейдите на вкладку «Архивация».
3. В меню «Задание» выберите команду «Создать». Раскройте узел «Мой компьютер», диск С:\, папка «Документы». Установите флажок напротив папки «Документы». Внизу, в поле «Носитель архива или имя файла» введите имя будущего архива -например С : \doc-normal. bkf. 5. Нажмите кнопку «Архивировать». Откроется окно «Сведения о задании архивации». В разделе «Если носитель уже содержит архивы» оставьте переключатель «Дозаписать этот архив к данным носителя».
4. Нажмите кнопку «Дополнительно». Убедитесь, что выбран тип архива «Обычный» и установите флажок «Проверка данных после архивации». Нажмите кнопку «ОК», а затем «Архивировать».

5. Откроется диалоговое окно «Ход архивации», и начнется процесс архивации. По завершении создания архива нажмите кнопку «Отчет» и посмотрите отчет. В нем не должно быть ошибок архивации. Закройте отчет и окно «Ход архивации». Не закрывайте программу Backup Windows.
6. Обратите внимание, что в папке C:\Документы теперь у всех файлов снят атрибут «архивный». Откройте файл Планы. txt и добавьте новую строку с текущей датой. Сохраните и закройте файл. Обратите внимание, что после внесения изменений в файл атрибут «архивный» автоматически устанавливается операционной системой.
7. Вернитесь к программе Backup Windows на вкладку «Архивация». В меню «Задание» выберите команду «Создать».
8. Раскройте узел «Мой компьютер», диск C:\, папка «Документы». Установите флажок напротив папки «Документы».
9. Внизу, в поле «Носитель архива или имя файла» введите имя добавочного архива – например C: \ doc-inc.bkf.
10. Нажмите кнопку «Архивировать». Откроется окно «Сведения о задании архивации».
1. Нажмите кнопку «Дополнительно». Выберите тип архива «добавочный» и установите флажок «Проверка данных после архивации». Нажмите кнопку «ОК».
2. Теперь кнопку «Расписание». Появится диалоговое окно, которое предложит вам сохранить заданные параметры, перед установкой архивации по расписанию. Нажмите кнопку «Да».
3. Сохраните набор ваших файлов под именем documents . bks.
4. В окне «Указание учетной записи» введите свой пароль и нажмите кнопку «ОК».
5. В появившемся окне «Параметры запланированного задания» введите имя задания – «Ежедневный добавочный архив».
6. Затем нажмите кнопку «Свойства».
7. Откроется окно «Запланированное задание», вкладка «Расписание». В выпадающем списке «Назначить задание» выберите вариант «ежедневно» и установите время начала на три минуты вперед от текущего времени, чтобы увидеть результат выполнения задания. Нажмите кнопку «ОК».
8. Введите повторно свой пароль и нажмите кнопку «ОК».
9. В окне «Параметры запланированного задания» также нажмите «ОК».
10. Перейдите на вкладку «Запланированные задания» программы архивации Backup и убедитесь, что ваше задание «Ежедневный добавочный архив» появилось в расписании (Каждый день, начиная с текущего).
11. Закройте программу Backup. Дождитесь наступления времени, установленного вами на запуск задания архивации. Вы увидите, как запустится по расписанию программа Backup. После ее выполнения на диске E появится добавочный архив doc-inc. bkf.
12. Запустите программу Backup. В меню «Сервис» выберите «Отчет». появится окно со списком отчетов архивации. Выберите последний и откройте его.
13. Сравните полученный отчет с предыдущим.
14. Закройте все окна программы Backup. Обратите внимание, что в папке C:\Документы опять у всех файлов снят атрибут «архивный».
15. Удалите папку «Документы» со всеми файлами.

Задание 2. Восстановите данные, ранее заархивированные, с помощью программы Backup.

1. Запустите программу Backup и перейдите на вкладку «Восстановление и управление носителем». В левом окне щелкните на узел «Файлы», чтобы раскрыть его. Выберите архив doc-normal. bkf.
2. Раскройте архив doc-normal .bkf и установите флажок напротив папки «Документы». Восстановим эту папку в ее исходное размещение. По умолчанию задан такой параметр снизу в выпадающем списке «Восстановить файлы в:».
3. Нажмите кнопку «Восстановить». В диалоговом окне «Подтверждение восстановления» нажмите кнопку «ОК».
4. В окне «Проверка расположения архивного файла» также нажмите кнопку «ОК».
5. После завершения восстановления закройте окно «Ход восстановления», нажав кнопку «Закрыть». Не закрывайте программу Backup Windows.

6. Убедитесь, что папка «Документы» со всеми файлами восстановлена в прежнее место на диск C:\. Откройте файл Планы. txt и убедитесь, что он не содержит последнюю строку текста с текущей датой.
7. Вернитесь в программу Backup на вкладку «Восстановление и управление носителем».
8. В левом окне щелкните и раскройте архив doc-inc.bkf и установите флажок напротив папки «Документы», в которой содержится один файл Планы. txt. По умолчанию программа Backup не заменяет существующие файлы с одинаковым именем. Поэтому необходимо сделать следующую настройку.
9. В меню «Сервис» выберите пункт «Параметры» и перейдите на вкладку «Восстановление». На этой вкладке переключитесь на вариант «Заменять файл на компьютере, только если он старее» и нажмите кнопку «ОК».
10. Нажмите кнопку «Восстановить». В диалоговом окне «Подтверждение восстановления» нажмите кнопку «ОК».
11. Если появится окно «Проверка расположения архивного файла», то так же нажмите кнопку «ОК».
12. После завершения восстановления закройте окно «Ход восстановления», нажав кнопку «Закрыть».
13. Закройте программу Backup Windows.
14. Убедитесь, что восстановлена последняя версия файла Планы. txt.

Задание 3. С помощью программы WinRar вы заархивируете данные и защитите архив паролем.

1. Создайте документ на диски С в папке Temp.
2. Загрузите программу – архиватор WinRar.
3. Перейдите в среде архиватора в созданную вами папку.
4. Создайте архив в вашей папке.
5. Перейдите на вкладку Дополнительно в среде архиватора. Выберите Установить пароль, задайте и подтвердите пароль.
6. Проверьте парольную защиту архива.

Устный опрос

1. Цель, задачи, предмет и основное содержание дисциплины, ее роль в системе подготовки студентов, а также в последующей практической деятельности.
2. Безопасность информации. Цель обеспечения защиты информации.
3. Система защиты информации.
4. Обеспечение защиты информации с точки зрения риска.
5. Критерии оценки защищенной системы. Общее решение задачи проектирования оптимальной системы защиты.
6. Нормативно-правовая база функционирования систем защиты информации.
7. Понятие угрозы. Классификация угроз.
8. Утечка, разглашение и несанкционированный доступ к конфиденциальной информации.
9. Характеристики информации.
10. Угрозы безопасности информации. Классификация методов и средств защиты информации.
11. Технические методы защиты.Задачи, решаемые техническими методами защиты. Методы решения данных задач.

Для устных ответов определяются следующие критерии оценок:

оценка «5» выставляется, если обучаемый:

- полно раскрыл содержание материала в объеме, предусмотренном программой и учебником;
- изложил материал грамотным языком в определенной логической последовательности, точно используя математическую и специализированную терминологию и символику;
- правильно выполнил графическое изображение алгоритма и иные чертежи и графики, сопутствующие ответу;

- показал умение иллюстрировать теоретические положения конкретными примерами, применять их в новой ситуации при выполнении практического задания;
- продемонстрировал усвоение ранее изученных сопутствующих вопросов, сформированность и устойчивость используемых при ответе умений и навыков;
- отвечал самостоятельно без наводящих вопросов учителя;

оценка «4» выставляется, если ответ имеет один из недостатков:

- в изложении допущены небольшие пробелы, не исказившие логического и информационного содержания ответа;
- нет определенной логической последовательности, неточно используется математическая и специализированная терминология и символика;
- допущены один-два недочета при освещении основного содержания ответа, исправленные по замечанию учителя;
- допущены ошибка или более двух недочетов при освещении второстепенных вопросов или в выкладках, легко исправленные по замечанию или вопросу учителя;

оценка «3» выставляется, если:

- неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса, имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, чертежах, блок-схем и выкладках, исправленные после нескольких наводящих вопросов учителя;
- ученик не справился с применением теории в новой ситуации при выполнении практического задания, но выполнил задания обязательного уровня сложности по данной теме,
- при знании теоретического материала выявлена недостаточная сформированность основных умений и навыков;

оценка «2» выставляется, если:

- не раскрыто основное содержание учебного материала;
- обнаружено незнание или непонимание учеником большей или наиболее важной части учебного материала,
- допущены ошибки в определении понятий, при использовании терминологии, в чертежах, блок-схем и иных выкладках, которые не исправлены после нескольких наводящих вопросов учителя.

Оценка («5», «4», «3») может ставиться не только за единовременный ответ (когда на проверку подготовки обучающегося отводится определенное время), но и за рассредоточенный во времени, т. е. за сумму ответов, данных обучающимся на протяжении урока (выводится поурочный балл), при условии, если в процессе урока не только заслушивались ответы обучающегося, но и осуществлялась проверка его умения применять знания на практике.

Раздел 2. Компьютерные вирусы и их защита.	ОК 02, ПК 11.2

Индивидуальное задание по теме «Изучение программных средств защиты от несанкционированного доступа»

Цель:

- изучить основные программные средства защиты от несанкционированного доступа;
- определить политику безопасности системы;
- научится применять некоторые средства защиты информации в ОС.

Задание:

1. Запустить программы просмотра и редактирования реестра Windows regedit.exe и regedt32.exe (с помощью команды «Выполнить» главного меню). Ознакомиться со структурой реестра.

1.1. Включить в отчет краткие сведения о содержании основных разделов реестра (HKEY_CURRENT_USER и HKEY_LOCAL_MACHINE).

1.2. Включить в отчет сведения о различиях в функциональных возможностях изученных программ редактирования реестра (если лабораторная работа выполняется в операционной системе Windows).

Примечание: в операционную систему Windows XP Professional включен один редактор реестра, который можно запустить с помощью любого из указанных выше имен.

Контрольные вопросы:

1. Какой из изученных в лабораторной работе редакторов реестра предоставляет функции по разграничению доступа к разделам реестра и как использовать эти функции?
2. Как с помощью программы restrick.exe ограничить доступ пользователей к дисковым устройствам?
3. Как ограничить доступ пользователей к функциям Панели управления с помощью программы restrick.exe?
4. Доступ к каким функциям Панели управления может быть ограничен с помощью программы restrick.exe?
5. В чем недостаточность средств ограничения прав пользователей, предоставляемых программой restrick.exe?
6. Как может быть заблокирована рабочая станция на период временного отсутствия пользователя? Укажите несколько вариантов.
7. Какой из способов блокирования рабочей станции на период временного отсутствия пользователя является наиболее безопасным и почему?

Индивидуальное задание по теме «Антивирусное программное обеспечение»

Цель: приобретение навыков защиты информации используя антивирусное программное обеспечение.

Задание. Изучить антивирусное программное обеспечение:

1. Программы-шпионы. Защита от программ шпионов.
2. Троянские программы.
3. «Черви», методики проникновения.
4. Вирусы, алгоритмы работы.
5. Антивирусное программное обеспечение:рекомендуемые настройки, правила использования.

Раздел3. Информационная безопасность вычислительных сетей.	ОК 04, ПК 11.6

Индивидуальное задание по теме «Средства безопасности ASP_NET. Аутентификация»

Цель:научиться создавать формы аутентификации, используя средства безопасности Asp_Net.

Задание. В рамках среды ASP.NET предоставлены 3 вида аутентификации:

- аутентификация Windows;
- формой;
- паспортом.

Контрольные вопросы:

1. Дайте определение аутентификации.
2. Дайте определение авторизации.
3. Какие вам известны способы аутентификации/идентификации?
4. Какие вам известны способы аутентификации с помощью средства безопасности Asp_Net?
5. В чем суть аутентификации Windows?
6. В чем суть аутентификации формой?

Индивидуальное задание по теме «Защита баз данных»

Цель: изучить способы защиты информации в БД на примере СУБД MS Access.

Задание. Создать новую базу данных и создать в ней следующие объекты:

- Таблицу Заказы.
- Запрос Сведения о заказах.
- Форму Заказы клиентов.

Заполнить таблицу несколькими записями.

Определить два уровня доступа к БД:

- на уровне пароля;

– на уровне пользователя (защита учетных записей пользователей и идентифицированных объектов).

Контрольные вопросы:

1. Способы защиты информации в БД Access.
2. Группы и пользователи БД Access. Файл рабочей группы.
3. Этапы создания рабочей группы с помощью мастера.
4. Порядок изменения пароля пользователя или группы.
5. Для чего создается связь защищенной на уровне пользователя базы данных с файлом рабочей группы (электронным ключом)?
7. К каким файлам БД относятся расширения *.mdw, *.bak, *.mdb?

Устный опрос по теме «Средства защиты компьютерной информации»

1. СредстваобеспеченияинформационнойбезопасностивInternet.
2. Историяразвития,структураи основныепонятиякриптологии.
3. Криптографиякак основаинформационнойбезопасности.
4. Подстановочныеиперестановочныекриптоалгоритмы.
5. Потоковыеиблочныекриптоалгоритмы.
6. Симметричныеиасимметричныекриптоалгоритмы.
7. Симметричныекриптосистемы.Общаясхемасимметричнойкриптосистемы.
8. Модельkриптосистемысоткрытымключом.Сертификацияоткрытыхключей.
9. АлгоритмсоткрытымключомRSA.
10. Электроннаяцифроваяподпись. Применениехэш-функции.
11. СтандартышифрованияDESиAES.
12. РоссийскийстандартшифрованияГОСТ28147-89.

Раздел4.Механизмы обеспечения «Информационной безопасности».	ОК 06, ПК 11.6

Индивидуальное задание по теме «Разработка простых криптографических алгоритмов на основе метода замены»

Цель: получение навыков создания простейшей криптосистемы симметричного шифрования.

Задание. В соответствии со своим вариантом разработать программу для шифрования русскоязычного текста при помощи шифра подстановки. Программы должны обеспечивать:

– шифрование информации, находящейся в текстовом файле, с записью результата в другой файл;
– шифрование информации, вводимой с клавиатуры, с выводом только шифр – текста;

Варианты заданий:

1. Шифр Цезаря.
2. Шифр Цезаря с ключевым словом.
3. Шифр Трисемуса.
4. Шифр Вижиненра.

Индивидуальное задание по теме «Разработка простых криптографических алгоритмов на основе метода перестановки»

Цель: получение навыков создания простейшей криптосистемы симметричного шифрования.

Варианты заданий:

1. Вывести сообщение с права на лево.
2. Простая шифрующая таблица перестановки.
3. Одиночная перестановка оп ключу.
4. Двойная перестановка по ключу.

Индивидуальное задание по теме«Шифрование информации с использованием стандарта DES»

Цель:

– получение навыков работы с пространством CryptoAPI для шифрования информации.
– разработка Web-приложения для шифрования информации с использование м стандарта DES.

Задание 1.Создайте новое Web-приложение:

1. Запустите Visual Studio и откройте пункт меню File.
2. В контекстном меню выберите New щелкните на Web Site. Когда вы выбираете этот значок, Visual Studio подготавливает среду разработки и файлы вашей программы для интернет-программирования. Создание нового проекта веб-приложения ASP.NET аналогично созданию проекта Windows Application. Однако текстовое поле Name (Имя) отключено, а текстовое поле Location (Расположение) предназначено для другого типа установки. В среде веб-приложения вам предлагается указать веб-сервер для вашего проекта или принять значение по умолчанию**http://localhost**. При создании проекта вы можете выбрать для него локальный или удаленный веб-сервер (на котором установлены .NET Framework и файлы поддержки), и Visual Studio будет использовать указанный веб-сервер для размещения и организации файлов вашего проекта. Веб-сервер определяется не с помощью имен диска и папки, а с помощью корректного адреса в интернете (URL).

Создайте Web-форму.

Как отмечалось ранее, Web Forms хранится в файле .aspx. В нашем случае это будет default.aspx. Для создания интерфейса мы можем:

– оставаться в окне редактора кода и формировать интерфейс с использование стандартных html-тэгов;
– перейти в режим конструктора и наполнить форму необходимыми компонентами.

Контрольные вопросы:

1. К какому методу шифрования относится криптостандарт DES?
2. Какое действие предполагает следующий участок кода:

```
Dim sr As New StreamReader(fs)

lblResult.Text = sr.ReadToEnd
```

3. В чем разница между шифрованием с использованием вектора инициализации и без него?
4. Укажите структуру инициализации криптопровайдера DES.

Индивидуальное задание по теме«Шифрование информации сиспользованием стандарта RSA»

Цель:

– получение навыков работы с пространством CryptoAPI для шифрования информации;
– разработка Web-приложения для шифрования информации с использование м стандарта RSA.

Задание. Создайте новое Web-приложение.Для создания интерфейса:

1. Оставаться в окне редактора кода и формировать интерфейс с использование стандартных html-тэгов.
2. Перейти в режим конструктора и наполнить форму необходимыми компонентами.
3. При использовании второго метода заполнения необходимо перейти в режим конструктора и перетащить на форму компоненты Button и 3 текстовых поля.
4. Отредактируйте свойства этих компонентов в соответствии со следующим кодом (для просмотра редактора перейдем в соответствующее окно кода нажав кнопку Sourse).

Контрольные вопросы

1. К какому методу шифрования относится криптостандарт RSA?
2. Укажите структуру инициализации криптопровайдера RSA.
3. Какое действие предполагает следующий участок кода:

```
        Private Enum KindOfAction As Integer
            RSAEncrypt = 0
            RSADecrypt = 1
        End Enum
End Class

End Namespace
```

4. Объясните причину того, что приложении может не с первого раза сработать корректно

Вопросы для устного опроса

1. Технологииилогикахраненияданных.
2. Стратегиязащитыивосстановленияданных.
3. Типыиметодырезервногокопирования.
4. Резервноекопированиефайловиобразов.Резервноекопированиепоплану.
5. Полное,дифференциальноеиинкрементноерезервноекопирование.
6. Безопасноехранениерезервныхкопий.
7. УстройствахраненияданныхТехнологияRAID.
8. Программыдлярезервногокопирования.Программыархивацииданных.
9. Настройкасистемныхпараметроврезервированияивосстановленияинформации.
10. Возможностирезервногокопирования.Оптимальныйпланвосстановленияипроверкаегоэффективности.
11. Настройкасистемныхпараметроврезервированияивосстановленияинформации.
12. Хранениеданныхв файловойсистемеFAT32. Хранениеданныхвфайловой системеNTFS.
13. Конфигурированиелогическихдисков.Монтированиедисков.
14. СредствадефрагментацииWindowsистороннихпроизводителей.
15. Инструментыдляработысразделамидисков.
16. Устранениепроблемсзагрузкойсистемы,файламиуправлениязагрузкойидрайверамиустройств.
17. СредствавосстановленияWindows.
18. Восстановлениеданныхпользователясистемы.
19. Восстановлениеданныхнажесткихдисках.

Промежуточная аттестация в виде комплексного дифференцированного зачета во 2 семестре	ОК 01, ОК 02, ОК 04, ОК 06, ПК 11.1, ПК 11.2, ПК 11.6

Вопросы к дифференцированному зачету

1. Понятие компьютерной информации. Виды ущерба компьютерной информации.Последствия причинения ущерба компьютерной информации.
2. Классификация угроз безопасности КИ. Потенциальные угрозы безопасностикомпьютерной информации, связанные с человеческим фактором.
3. Логическая организация дискового пространства. Понятие о «технологическом» мусоре в памяти ПЭВМ
4. Классификация и механизмы действия вирусных программ.
5. Аппаратура персонального компьютера и безопасность информации.
6. Факторы, способствующие реализации угроз безопасности компьютерной информации.
7. Понятие безопасности компьютерной информации. Принципы защиты информации.
8. Понятие политики безопасности компьютерных систем, ее основные составляющие.
9. Методы защиты информации в компьютерных системах.
10. Одноуровневая модель разграничения доступа, достоинства и недостатки.
11. Многоуровневаямодельразграничениядоступа,достоинстваи недостатки.
12. Реализация политики разграничения доступа в ОС Windows.
13. Понятие механизмов идентификации и аутентификации, их реализация в ОС Windows.
14. Классическаясхемакриптографическойзащитыинформации. Ее достоинства и недостатки. Примеры симметричных криптоалгоритмов.
15. Схема криптографической защиты информации с открытым ключом. Ее достоинства и недостатки. Примеры асимметричных криптоалгоритмов.
16. Схема использования электронной цифровой подписи. Понятие хеш-функции.
17. Файловая система FAT с точки зрения обеспечения информационной безопасности.
18. Основные свойства файловой системы NTFS. Структура NTFS.

19. Понятие об MFT. Структура записи в MFT.
20. Организация резидентных файлов в NTFS. Возможность восстановления удаленных резидентных файлов.
21. Организация нерезидентных файлов в NTFS. Возможность восстановления удаленных нерезидентных файлов.
22. Архивирование и резервирование компьютерной информации. Типы архивов.
23. Ротация внешних носителей информации. Стратегии архивирования.
24. Применениеспециализированныхпрограммныхсредствзащиты информации, их достоинства и недостатки.
25. Физические носители кодов паролей.
26. Требования к специализированным средствам защиты информации от несанкционированного доступа.
27. Организация виртуальных логических дисков.
28. Механизмы организации контроля доступа до загрузки ОС. Механизмы доверенной загрузки ОС, реализованные в СЗИ

Итоговый тест

1) К правовым методам, обеспечивающим информационную безопасность, относятся:
- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
+ Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:
- Хищение жестких дисков, подключение к сети, инсайдерство
+ Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:
+ Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:
+ несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций

5) Основные объекты информационной безопасности:
+ Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:
- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
+ Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:
+ Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:
- руководители, менеджеры, администраторы компаний
+ органы права, государства, бизнеса
- сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:
+ Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компании

- Внедрение аутентификации, проверки контактных данных пользователей

тест 10) Принципом информационной безопасности является принцип недопущения:

+ Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности

11) Принципом политики информационной безопасности является принцип:

+ Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:

+ Усиления защищенности самого незащищенного звена сети (системы)
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип:

+ Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:

- Компьютерный сбой
+ Логические закладки («мины»)
- Аварийное отключение питания

15) Когда получен спам по e-mail с приложенным файлом, следует:

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

16) Принцип Кирхгофа:

- Секретность ключа определена секретностью открытого сообщения
- Секретность информации определена скоростью передачи данных
+ Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:

- Электронно-цифровой преобразователь
+ Электронно-цифровая подпись
- Электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:

- Покупка нелицензионного ПО
+ Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:

- Распределенный доступ клиент, отказ оборудования
- Моральный износ сети, инсайдерство
+ Сбой (отказ) оборудования, нелегальное копирование данных

тест_20) Наиболее распространены средства воздействия на сеть офиса:

- Слабый трафик, информационный обман, вирусы в интернет
+ Вирусы в сети, логические мины (закладки), информационный перехват
- Компьютерные сбои, изменение администрирования, топологии

21) Утечкой информации в системе называется ситуация, характеризуемая:

+ Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

+ Целостность
- Доступность

- Актуальность

23) Угроза информационной системе (компьютерной сети) – это:

+ Вероятное событие
- Детерминированное (всегда определенное) событие
- Событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:

- Регламентированной
- Правовой
+ Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке:

+ Программные, технические, организационные, технологические
- Серверные, клиентские, спутниковые, наземные
- Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:

+ Владелец сети
- Администратор сети
- Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:

+ Руководств, требований обеспечения необходимого уровня безопасности
- Инструкций, алгоритмов поведения пользователя в сети
- Нормы информационного права, соблюдаемые в сети

28) Наиболее важным при реализации защитных мер политики безопасности является:

- Аудит, анализ затрат на проведение защитных мер
- Аудит, анализ безопасности
+ Аудит, анализ уязвимостей, риск-ситуаций