Государственное образовательное учреждение
**«Приднестровский государственный университет им. Т.Г.Шевченко»**
**Инженерно-технический институт**

**Кафедра государственного управления**

УТВЕРЖДАЮ
Зав. кафедрой ГУ,доцент
А.Г. Мафтей

«10» сентября2020 г.

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ**
**по дисциплине**

# Б1.В.ДВ.04.01 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ»

Направление подготовки
**5.38.04.04 «Государственное и муниципальное управление»**

Профиль (специализация) подготовки
**Публичное управление**

Квалификация (степень) выпускника: **магистр**

Форма обучения: **очная, заочная**

Год набора: **2020 г.**

Разработал: доцент

А.Ю. Долгов

Тирасполь, 2020

**Паспорт фонда оценочных средств по учебной дисциплине.**

**1. В результате изучения «Информационная безопасность и защита информации» у обучающихся должны быть сформированы следующие компетенции:**

| Категория (группа) компетенций | Код и наименование | Код и наименование индикатора достижения универсальной компетенции |
|---|---|---|
| ***Общепрофессиональные компетенции и индикаторы их достижения*** | | |
| | ПК-1. владение технологиями управления персоналом, обладанием умениями и готовностью формировать команды для решения поставленных задач | ИД-1$_{ПК-1}$<br>Знать: основные понятия информационной безопасности, основные принципы организации и алгоритмы функционирования операционных систем и оболочек |
| | | ИД-2$_{ПК-1}$<br>Уметь: ориентироваться в современной системе источников информации |
| | | ИД-3$_{ПК-1}$<br>Владеть: навыками поиска информации в глобальной информационной сети Интернет, работы с базами данных и Интернет-ресурсами |
| | ПК-2. владение организационными способностями, умение находить и принимать организационные управленческие решения, в том числе и в кризисных ситуациях | ИД-1$_{ПК-2}$<br>Знать: возможности применения в работе современных системных программных средств: операционных систем, операционных оболочек, обслуживающих программ |
| | | ИД-2$_{ПК-2}$<br>Уметь: использовать современные информационные технологии в своей профессиональной деятельности |
| | | ИД-3$_{ПК-2}$<br>Владеть: навыками современной терминологии и методологии в области информационной безопасности |
| | ПК-8. владение принципами и современными методами управления операциями в различных сферах деятельности | ИД-1$_{ПК-8}$<br>Знать: основные принципы организации и алгоритмы функционирования систем безопасности в современных операционных системах и оболочках |
| | | ИД-2$_{ПК-8}$<br>Уметь: пользоваться программными средствами, реализующими основные криптографические функции - системы публичных ключей, цифровую подпись, разделение доступа |
| | | ИД-3$_{ПК-8}$<br>Владеть: навыками применения аппаратных и программных средств обеспечения информационной безопасности |
| | ПК-10. способность вырабатывать решения, учитывающие правовую и нормативную базу | ИД-1$_{ПК-10}$<br>Знать: правовые акты в области защиты государственной тайны и информационной безопасности |
| | | ИД-2$_{ПК-10}$<br>Уметь: видеть и формулировать проблему, видеть конкретную ситуацию, прогнозировать и предвидеть, рассчитывать риски, ставить цели и задачи |
| | | ИД-3$_{ПК-10}$<br>Владеть: навыками противостояния типовым удаленным атакам |

**2. Программа оценивания контролируемой компетенции:**

| Текущая аттестация | Контролируемые модули, разделы (темы) дисциплины и их наименования | Код контролируемой компетенции или его части | Наименование оценочного средства |
|---|---|---|---|
| РУБЕЖНЫЙ КОНТРОЛЬ | Информация и информационные ресурсы | ПК-1, ПК-2 | ПЗ1, ПЗ2, ПЗ3 |
| РУБЕЖНАЯ АТТЕСТАЦИЯ | Безопасность информационных систем Основы защиты информации | ПК-8, ПК-10 | КТ, ПЗ4, ПЗ5, ПЗ6 |
| Промежуточная аттестация | | Код контролируемой компетенции или его части | Наименование оценочного средства |
| | | ПК-1, ПК-2, ПК. ПК-8, ПК10 | зачет |

**3. Показатели и критерии оценивания компетенции по этапам формирования, описание шкал оценивания**

| Этапы оценивания компетенции | Показатели достижения заданного уровня освоения компетенции | Критерии оценивания результатов обучения | | | |
|---|---|---|---|---|---|
| | | **2** | **3** | **4** | **5** |
| Первый этап | ИД-1$_{ПК-1}$ **Знать:** основные понятия информационной безопасности, основные принципы организации и алгоритмы функционирования операционных систем и оболочек | Не знает | Знает основные понятия теории информационной безопасности, но не знает основные принципы организации и алгоритмы функционирования операционных систем и оболочек | Знает основные понятия и основы теории, а также имеет представление об информационной безопасности, но не может применить один из принципов организации и алгоритмов функционирования операционных систем и оболочек | Знает основные понятия информационной безопасности, основные принципы организации и алгоритмы функционирования операционных систем и оболочек |

| | | | | | |
|---|---|---|---|---|---|
| Второй этап | ИД-2$_{ПК-1}$ **Уметь**: ориентироваться в современной системе источников информации | Не умеет | Правильно решает стандартные профессиональные задачи с применением знания о современной системе источников информации, но затрудняется применить на практике навыки работы с универсальными и специальными пакетами прикладных программ | Умеет использовать в практической деятельности знания о современной системе источников информации, применять на практике навыки работы с некоторыми универсальными и специальными пакетами прикладных программ | Умеет ориентироваться в современной системе источников информации |
| Третий этап | ИД-3$_{ПК-1}$ **Владеть:** навыками поиска информации в глобальной информационной сети Интернет, работы с базами данных и Интернет-ресурсами | Не владеет | Владеет частью навыков поиска информации в глобальной информационной сети Интернет, работы с базами данных и Интернет-ресурсами, но исключительно в привычной среде для решения узких профессиональны х задач | Владеет частью навыков поиска информации в глобальной информационной сети Интернет, работы с базами данных и Интернет-ресурсами | Владеет навыками поиска информации в глобальной информационной сети Интернет, работы с базами данных и Интернет-ресурсами |
| Первый этап | ИД-1$_{ПК-2}$ **Знать:** возможности применения в работе современных системных программных средств: операционных систем, операционных оболочек, обслуживающих программ | Не знает | Знает основные один из способов построения, методы создания и принципы проектирования информационных технологий и компьютеризированных систем управления, но не знает архитектуру информационных систем управления организации | Знает основные понятия и способы построения, методы создания и принципы проектирования информационных технологий и компьютеризированных систем управления, слабо представляет архитектуру информационных систем управления организации | Знает методические основы построения, методы создания и принципы проектирования информационных технологий и компьютеризированных систем управления, а также архитектуру информационных систем управления организации |

| | | | | | |
|---|---|---|---|---|---|
| Второй этап | ИД-2$_{ПК-2}$ **Уметь:** использовать современные информационные технологии в своей профессиональной деятельности | Не умеет | Правильно применяет на практике отдельные принципы построения современных информационных систем, офисных систем, но не умеет применять информационные технологии для решения управленческих задач | Умеет применять на практике только некоторые принципы построения современных информационных систем, офисных систем, обрабатывать эмпирические и экспериментальные данные, но не умеет устанавливать и руководить установкой сетевого программного обеспечения | Умеет применять на практике принципы построения современных информационных систем, офисных систем, обрабатывать эмпирические и экспериментальные данные, применять информационные технологии для решения управленческих задач |
| Третий этап | ИД-3$_{ПК-2}$ **Владеть:** навыками современной терминологии и методологии в области информационной безопасности | Не владеет | Владеет частью навыков работы в глобальных компьютерных сетях и корпоративных информационных системах, но не владеет навыками работы с пакетами программ для решения исследовательских задач, навыками математических, статистических и количественных методов решения типовых управленческих задач | Владеет навыками работы в глобальных компьютерных сетях и корпоративных информационных системах, а также частичными навыками работы с пакетами программ для решения исследовательских задач, навыками математических, статистических и количественных методов решения типовых управленческих задач | Владеет навыками работы в глобальных компьютерных сетях и корпоративных информационных системах, работы с пакетами программ для решения исследовательских задач, навыками математических, статистических и количественных методов решения типовых управленческих задач |
| Первый этап | ИД-1$_{ПК-8}$ **Знать:** основные принципы организации и алгоритмы функционирования систем безопасности в современных операционных системах и оболочках | Не владеет | Знает основные один из способов организации и алгоритмов функционировани я систем безопасности в современных операционных системах и оболочках, но не знает архитектуру информационных систем безопасности организации | Знает основные понятия и способы организации и алгоритмы функционирования систем безопасности в современных операционных системах и оболочках, слабо представляет архитектуру информационных систем безопасности организации | Знает основные принципы организации и алгоритмы функционирования систем безопасности в современных операционных системах и оболочках |

| | | | | | |
|---|---|---|---|---|---|
| Второй этап | ИД-2$_{ПК-8}$<br>**Уметь:**<br>пользоваться программными средствами, реализующими основные криптографические функции - системы публичных ключей, цифровую подпись, разделение доступа | Не владеет | Правильно применяет на практике отдельные программные средства, реализующие основные криптографически е функции, офисных систем, но не умеет применять специальное программное обеспечение для цифровой подписи и разделения доступа | Умеет применять на практике только некоторые программные средства, реализующие основные криптографические функции - системы публичных ключей, цифровую подпись, разделение доступа, но не умеет устанавливать и руководить установкой специального программного обеспечения | Умеет пользоваться программными средствами, реализующими основные криптографические функции - системы публичных ключей, цифровую подпись, разделение доступа |
| Третий этап | ИД-3$_{ПК-8}$<br>**Владеть:**<br>навыками применения аппаратных и программных средств обеспечения информационной безопасности | Не владеет | Владеет частью навыков применения либо аппаратных, либо программных средств обеспечения информационной безопасности, но не владеет навыками работы с пакетами специальных программ для решения задач обеспечения информационной безопасности | Владеет навыками применения либо аппаратных, либо программных средств обеспечения информационной безопасности, а также частичными навыками работы с пакетами специальных программ для решения задач обеспечения информационной безопасности | Владеет навыками применения аппаратных и программных средств обеспечения информационной безопасности |
| Первый этап | ИД-1$_{ПК-10}$<br>**Знать:**<br>правовые акты в области защиты государственной тайны и информационной безопасности | Не владеет | Знает некоторые правовые акты в области защиты государственной тайны и информационной безопасности, но не знает правоприменитель ную практику в области систем информационной безопасности | Знает основные правовые акты в области защиты государственной тайны и информационной безопасности, слабо представляет правоприменительн ую практику в области систем информационной безопасности | Знает правовые акты в области защиты государственной тайны и информационной безопасности |

| | | | | | |
|---|---|---|---|---|---|
| Второй этап | ИД-2$_{ПК-10}$ **Уметь:** видеть и формулировать проблему, видеть конкретную ситуацию, прогнозировать и предвидеть, рассчитывать риски, ставить цели и задачи | Не владеет | Правильно видит и формулирует проблему, видеть конкретную ситуацию, но не умеет ставить цели и задачи, прогнозировать, предвидеть и рассчитывать риски информационной безопасности | Умеет видеть и формулировать проблему, видеть конкретную ситуацию, ставить цели и задачи, но не умеет прогнозировать, предвидеть и рассчитывать риски информационной безопасности | Умеет видеть и формулировать проблему, видеть конкретную ситуацию, прогнозировать и предвидеть, рассчитывать риски, ставить цели и задачи |
| Третий этап | ИД-3$_{ПК-10}$ **Владеть:** навыками противостояния типовым удаленным атакам | Не владеет | Владеет частью навыков противостояния типовым удаленным атакам, но не владеет навыками работы с пакетами специальных программ для решения задач обеспечения информационной безопасности | Владеет навыками противостояния типовым удаленным атакам, а также частичными навыками работы с пакетами специальных программ для решения задач обеспечения информационной безопасности | Владеет навыками противостояния типовым удаленным атакам |

***4.*** **Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций при изучении учебной дисциплины в процессе освоения образовательной программы**

4.1 Типовой вариант задания на контрольную работу

4.2. Типовой вариант задания на практическую работу

**Защита документов MS Word.**

***Задание 1.*** Создать шаблон делового письма с защищенными от изменения реквизитами.

1. Создать новый документ Word, вставив в нужном месте графический элемент – линию, для этого:

- создать новый документ и сохранить его с именем «Письмо». Ввести и отформатировать текст документа в соответствии с рис.1.
- Добавить пустую строку между реквизитами организации и исходящим номером письма, установить для нее форматирование абзаца без отступов по бокам, без красной строки, выравнивание: по центру;
- Установить курсор в начало пустой строки и вставить графическую линию, выполнив команду *Вставка*|*Клип*. В области команды нажать кнопку *Поиск*, выделить изображение понравившейся линии в коллекции клипов и щелкнуть по нему мышью для вставки в документ.
- Закрыть область вставки клипов.

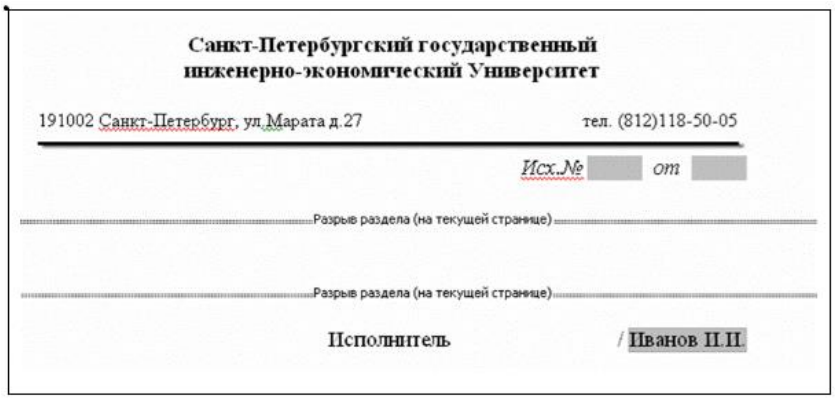



*Рис.1. Текст шаблона стандартного письма*

2. После слов «Исх.№», «от» и «/» ввести поля формы для занесения данных в защищенном от изменения документе. Для этого следует сначала настроить приложение MS Word для работы с элементами управления форм:

- В строке меню MS Word появится вкладка *Разработчик*.
- На вкладке *Разработчик* в группе *Элементы управления* нажать кнопку *Режим конструктора*.
- Установить курсор после слов «Исх.№ », затем щелкнуть элемент управления *Форматированный текст*  для ввода произвольного текста.
- Аналогичным образом следует вставить элемент управления *Дата*  после слова «от » для выбора даты;
- После слов «Исполнитель /» вставить элемент управления *Раскрывающийся список*  для выбора фамилии исполнителя из списка.
- После вставки поля *Раскрывающийся список* следует задать варианты для выбора (элементы списка). Для того, чтобы задать элементы списка, следует выделить вставленный элемент списка, щелкнув на нем мышью, а затем нажать кнопку *Свойства*  в группе *Элементы управления*.
- В окне свойств списка (рис.2) нажать кнопку *Добавить* и ввести в окне *Добавить вариант фамилию первого исполнителя*, нажать *ОК*. Затем добавить еще две-три фамилии исполнителей. Удалить пункт *«Выберите элемент»* из значений списка, для чего следует выделить данный вариант мышью, а затем нажать кнопку *Удалить*.
- Задать написание фамилии исполнителя курсивом. Для этого в окне свойств списка установить флажок *Использовать стиль для форматирования содержимого*, затем щелкнуть на кнопке *Создать стиль* и создать новый стиль, основанный на стиле абзаца, с написанием курсивом. Для сохранения стиля нажать *ОК*. Для выхода из окна нажать *ОК*.

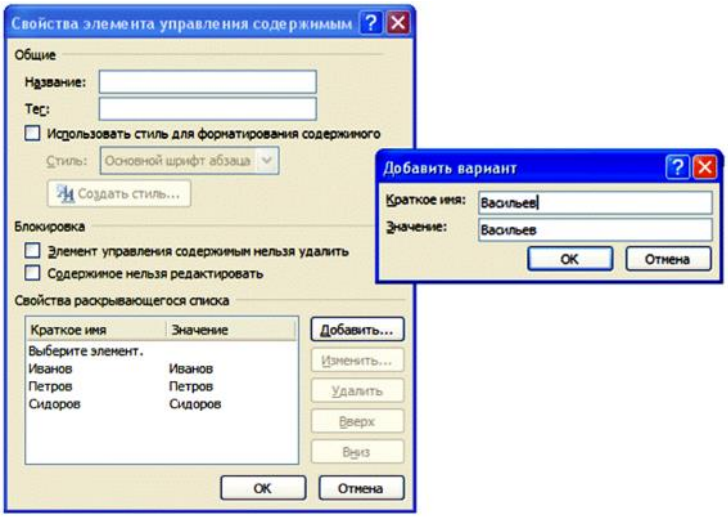



*Рис.2. Формирование списка исполнителей*

3. Проверить действие текстового поля, поля и поля со списком (возможен ввод текста, выбор даты, выбор из списка). Если поля не действуют, следует нажать кнопку *Режим конструктора*.

4. Разбить документ на три части (раздела) в соответствии с рис.3:
первый раздел – содержит шапку письма с исходящим номером и датой создания письма;
второй раздел – пустые строки в середине письма, предназначенный для набора текста письма;
третий раздел – включающий подпись и фамилию исполнителя.

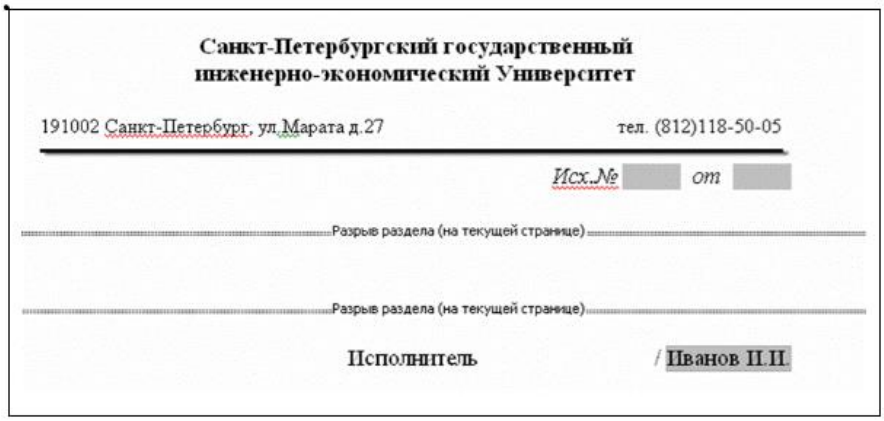



*Рис.3. Разбиение документа шаблона письма на разделы*

Для того, чтобы вставляемые линии разрывов отображались на экране, на вкладке *Главная* следует включить режим отображения непечатаемых символов – нажать кнопку ¶.
Вставить два разрыва раздела (первый – после строки с исходящим номером, второй – перед словом «Исполнитель»), оставив между ними пустые строки. Для вставки разрыва:

- установить курсор в место вставки разрыва;
- перейти на вкладку *Разметка страницы* и открыть группу *Разрывы*. В группе *Разрывы* выбрать *Разрывы разделов/ Текущая страница*.

5. Установить защиту от изменения текста первого и третьего разделов документа, содержащих шапку и подпись стандартного письма с паролем ***high***:

- На вкладке *Разработчик* или *Рецензирование* открыть группу *Защита*, выбрать команду *Ограничить редактирование*
- в области команды *Ограничить форматирование и редактирование* установить флажок *Разрешить только указанный способ редактирования документа* в группе *Ограничения на редактирование* и выбрать из выпадающего списка *Ввод данных в поля форм*.
- Затем щелкнуть мышью на появившейся ссылке *Выбор разделов* и установить флажки только напротив разделов 1 и 3 (рис.4), подтвердить выбор защищаемых разделов, нажав *ОК*.

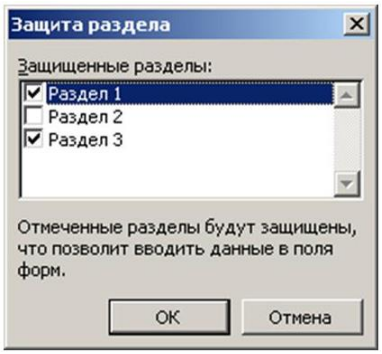



*Рис.4. Установка защиты отдельных разделов документа*

- Активировать введенные ограничения, щелкнув на кнопке *Да*, включить защиту, дважды ввести пароль ***high*** (в поле ввода пароля и поле подтверждения), нажать *ОК*.

- Проверить, что защита установлена, то есть можно менять только текст содержимого письма (Раздел 2 документа), а также менять значения элементов управления в шапке письма и выбирать фамилию исполнителя из списка.

6. Установить парольную защиту просмотра документа «Письмо» с помощью пароля на открытие (пароль ***low***):

- Откройте вкладку *Файл*.
- Щелкните элемент *Сведения*.
- Щелкните *Защитить документ → Зашифровать паролем*.
- В поле *Шифрование документа* введите пароль и нажмите кнопку *ОК*.
- Еще раз введите пароль в поле *Подтверждение пароля* и нажмите кнопку *ОК*.

7. Сохранить документ «Письмо». Проверить действие парольной защиты, закрыв и заново открыв документ.

8. Установить для документа «Письмо» режим «только чтение» или Разрешение записи, защищенный паролем. Для этого:
Выполнить команду *Файл → Сохранить как*, щелкнуть на кнопке *Сервис* и выбрать пункт *Общие параметры*. В окне общих параметров уже задан пароль для открытия файла (отображается черными точками), поставить галочку в окне *«Рекомендовать доступ только для чтения»* или ввести пароль *medium* в строку пароль разрешения записи. Нажать *ОК*, а затем ввести *medium* еще раз в строке подтверждения ввода пароля. Затем нажать кнопку *Сохранить* в окне сохранения документа.

9. Проверить действие пароля разрешения записи, закрыв и вновь открыв документ «Письмо».

***Задание 2.*** На основе общего шаблона письма создать шаблон делового письма конкретного исполнителя.
10. Открыть документ «Письмо», выполнить команду *Сохранить как*, в окне команды ввести новое имя файла *«Письмо1»*, рекомендовать для нового файла открытие в режиме «только чтение», удалив в группе *Сервис/Общие параметры* пароль разрешения записи и установив флажок *Рекомендовать доступ только для чтения*.

11. Проверить действие новых параметров, закрыв и вновь открыв документ *«Письмо1»*. При открытии документа его следует открыть в режиме записи изменений, ответив во втором окне предупреждения *НЕТ*.

12. Ввести номер, выбрать дату и фамилию исполнителя в полях документа. Занести произвольный текст письма. В конце текста письма набрать строку текста: «Последнее изменение» и вставить текущую дату и время, щелкнув на кнопке Дата и время  группы *Текст* на вкладке *Вставка*. Выбрать формат даты с указанием числа и времени с точностью до секунд. Включить флажок *Обновлять автоматически*. Для вставки поля даты в документ нажать *ОК*.

13. Проверить действие поля даты. Запомнить вставленное значение времени (минуты, секунды). Сохранить документ. Затем закрыть и заново открыть документ в режиме записи изменений (см.п.11). Проверить, что значение времени последнего изменения документа изменилось.

14. Запретить изменение фамилии исполнителя. Для этого:

- Снять защиту частей документа «Письмо1», щелкнув в окне команды *Рецензирование/Защитить документ/Ограничить форматирование и редактирование* кнопку *Отключить защиту*.
- Выделить поле с фамилией исполнителя, щелкнув на ней мышью. На вкладке *Разработчик* щелкнуть на кнопке *Свойства*. В окне свойств элемента управления включить флажки *Элемент управления содержимым нельзя удалить* и *Содержимое нельзя редактировать*.
- Проверить действие установленных флажков.

15. Установить защиту первого и третьего разделов документа «Письмо1» с паролем ***high***. Сохранить изменения в документе.

***Задание 3.*** Создать окончательную версию делового письма, заверенную цифровой подписью исполнителя.

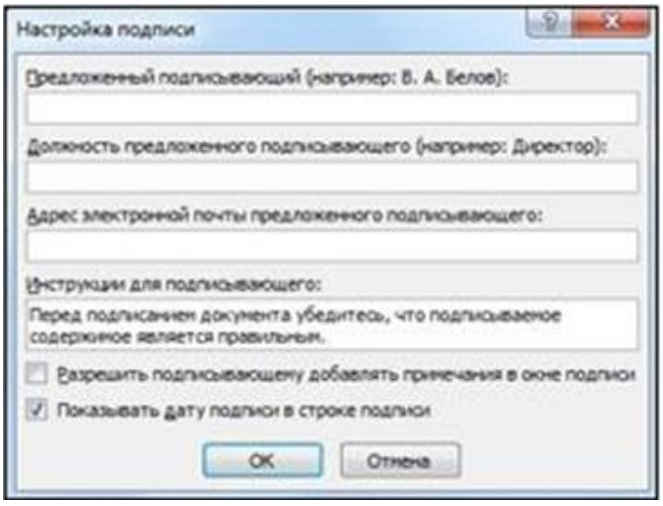
16. Открыть документ «Письмо1» и сохранить его под новым именем «Письмо 2», оставив из ограничений доступа только пароль на открытие документа (в окне команды *Сохранить как/Сервис/Общие параметры* снять флажок *Рекомендовать доступ только для чтения*).

17. Окончательно отредактировать текст документа (при необходимости сменить дату письма на актуальную). Отключить защиту разделов внутри документа «Письмо2».

18. Просмотреть свойства документа и убедиться, что были очищены все свойства на вкладке Документ.

19. Создать собственный цифровой сертификат: в *Главном меню Windows (Пуск/Программы)* выбрать в группе *MicrosoftOffice/Средства MicrosoftOffice (Microsoft Office Tools)* средство *Цифровой сертификат для проектов VBA(Digital Certificate for VBA Projects)*, и ввести в строку создания сертификата свое имя.

20. Заверить документ «Письмо2» своей цифровой подписью. Для этого:
1. Поместите указатель мыши в то место в документе, где необходимо создать строку подписи.
2. На вкладке *Вставка* в группе *Текст* раскройте список *Строка подписи* и выберите пункт *Строка подписи Microsoft Office*.
3. В диалоговом окне *Настройка подписи* введите сведения, которые будут под строкой подписи.
4. Предложенный подписывающий. Полное имя подписывающего лица.




5. Должность подписывающего лица (если таковая имеется).
6. Адрес электронной почты подписывающего лица (при необходимости).
7. Инструкции для подписывающего лица.
8. Установите оба указанных ниже флажка.

4.3 Типовой тест промежуточной аттестации

1. Дайте определение понятия «информация».

1) Информация – это набор взаимосвязанных компонентов, функционирующих совместно для достижения определенной цели.

+2) Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

3) Информация – это зафиксированные на материальном носителе сведения с реквизитами, позволяющими их идентифицировать.

2. Что представляет собой информатизация?

1) Информатизация – это комплекс, который включает компьютерное и коммуникационное оборудование, программное обеспечение, лингвистические средства, информационные ресурсы, а также системный персонал, обеспечивающий поддержку динамической информационной модели некоторой части реального мира для удовлетворения информационных потребностей пользователей и для принятия решений.

2) Информатизация – это процесс сбора, обработки, накопления, хранения, поиска и распространения информации.

+3) Информатизация – это организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав юридических и физических лиц на основе формирования и использования информационных ресурсов. Информатизация базируется на применении автоматизированных информационных технологий (АИТ).

3. Что представляет собой документированная информация (документ)?

-1) Документированная информация (документ) – это организационно упорядоченная совокупность документов (массивов документов) и информационных технологий.

2) Документированная информация (документ) – набор взаимосвязанных компонентов, функционирующих совместно для достижения определенной цели.

+3) Документированная информация (документ) – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

4. Что представляют собой информационные ресурсы?

1) Система – это комплекс, который включает компьютерное и коммуникационное оборудование, программное обеспечение, лингвистические средства, информационные ресурсы.

+2) Под системой понимают набор взаимосвязанных компонентов, функционирующих совместно для достижения определенной цели.

-3) Система представляет собой инфраструктуру, обеспечивающую реализацию информационных процессов сбора, обработки, накопления, хранения, поиска и распространения информации.

5. Что представляет собой информационная революция?

1) Информационная революция – это радикальное, коренное, глубокое, качественное изменение, скачок в развитии общества, природы или познания, сопряжённое с открытым разрывом с предыдущим состоянием.

+2) Информационная революция – это преобразования общественных отношений из-за кардинальных изменений в сфере обработки информации. Следствием подобных преобразований являлось приобретение человеческим обществом нового качества.

3) Информационная революция – это коренное качественное преобразование производительных сил, качественный скачок в структуре и динамике развития производительных сил.

6. Когда произошла и с чем связана четвертая информационная революция?

1) Четвертая информационная революция произошла в 60-х гг. XX века и связана с появлением микроэлектроники, приведший к модульному принципу построения компьютеров. В результате возросло количество и производительность суперкомпьютеров, увеличился объем обрабатываемой информации.

2) Четвертая информационная революция произошла в 90-х гг. XX века и связана с появлением глобальной сети передачи данных интернет. После этого появились глобальные вычислительные сети и параллельные суперкомпьютеры с разделяемой памятью.

+3) Четвертая информационная революция произошла в 70-х гг. XX века и связана с появлением микропроцессорной техники и, в частности, персональных компьютеров. Вскоре после этого возникли компьютерные телекоммуникации, радикально изменившие системы хранения и поиска информации.

7. Что такое государственные информационные ресурсы?

1) *Государственные информационные ресурсы* – это комплексная информационная ресурсная система, предназначенная для информационно-аналитической поддержки органов государственного управления.

2) *Государственные информационные ресурсы* – это ресурсы, находящиеся в собственности или распоряжении или владении и пользовании всех юридических и физических лиц, находящихся под юрисдикцией определённого государства.

+3) *Государственные информационные ресурсы* – это ресурсы, которые находятся в ведении государственных органов власти, органов власти районных и муниципальных и в их совместном ведении.

8. Кто ввел понятие «информационное общество»?

1) Понятие "информационное общество" в середине 70-х годов XX века ввел американский ученый космолог А. Хартман из Оклендского университета.

+2) Понятие "информационное общество" возникло во второй половине 1960-х гг. Считается, что его изобретением мы обязаны профессору Токийского технологического университета Ю. Хаяши.

3) Понятие "информационное общество" в конце XX века ввел японский исследователь в области социальных перспектив современного общества профессор Киотского университета С. Кабаяши.

9. Что понимают под термином «информационное общество»?

1) Под термином «информационное общество» понимают такой социальный строй, при котором главной ценностью является определенное количество накопленной информации и возможность контролировать ее потоки.

2) Под термином «информационное общество» понимают такую общественно-политическую формацию, при которой информационное содержание каждого производимого продукта составляет не мене 50% его стоимости, а средства обработки информации распределены между членами общества.

+3) Под «информационным обществом» понимается такое общество, в котором главным условием благополучия каждого человека и каждого государства становится знание, полученное благодаря беспрепятственному доступу к информации и умению работать с ней, а сам информационный обмен не имеет ни временных, ни пространственных, ни политических границ.

10. Перечислите основные признаки «информационного общества».

(Внимание! Множественный ответ)

+1) Наличие внутреннего информационного рынка, а также его интеграция с мировым информационным рынком.

+2) Полноценное развитие информационной инфраструктуры, обеспечивающей возможность доступа к отечественным и зарубежным информационным ресурсам (порталы, терминалы, банки данных, компьютерные сети и др.).

3) Появление новых рабочих мест, автоматизация производства, существенные сдвиги происходят в сфере занятости и трудоустройства.

+4) Существование высокого уровня международного информационного обмена, т.е. характер взаимодействия с другими странами, а также собственного влияния на мировую экономику информационных товаров и услуг.

5) Свобода доступа к информации влияет на политический процесс, что связано с возможностью "электронного" голосования и "электронного" правосудия.

11. На какие области позволяет влиять «информационная экономика»?

(Внимание! Множественный ответ)

1) На естественно-научную сферу (появление новых знаний о человеке и окружающей среде, расшифровка и извлечение древних знаний, исследование других миров, существенное продвижение в изучении строения атомного ядра).

+2) На техническую сферу (широкое внедрение информационных технологий в производство, быт, образование)

+3) На социальную сферу (появление новых рабочих мест, автоматизация производства, существенные сдвиги происходят в сфере занятости и трудоустройства).

4) На инновационную сферу (обеспечивающее повышение эффективности процессов и (или) улучшение качества продукции, востребованное рынком).

+5) На экономическую сферу (научно-техническая информация все шире включается в товарно-денежные отношения; информационные продукты превращаются в основной экономический ресурс наравне с оборотом товаров и услуг, становятся источником прибыли; информация существенно влияет на качество жизни населения планеты).

+6) На политическую сферу (свобода доступа к информации влияет на политический процесс, что связано с возможностью "электронного" голосования и "электронного" правосудия).

7) На технологическую сферу (создание новых материалов и технологий, роботизация промышленного производства, замена ручного труда машинным).

+8) На гуманитарную сферу (формируется новое информационное сознание, связанное с изменением системы норм и ценностей, отвечающих потребностям развития отдельного индивида и общества в целом).

12. Перечислите направления деятельности, связанные с информационным обслуживанием населения.

(Внимание! Множественный ответ)

1) информационное обеспечение социальной защиты населения.

+2) информационное обеспечение системы государственного управления.

+3) информационное обеспечение образования (обучение дистанционным способом, либо с применением электронных и дистанционных технологий).

4) информационное обеспечение системы перинатальных услуг и центров.

+5) информационное обеспечение системы здравоохранения (медицинская информатика).

6) информационное обеспечение наукоемкого гражданского производства.

13. Перечислите этапы распространения новых информационных технологий.

(Внимание! Множественный ответ)

+1) Возникновение различных форм автоматизированной обработки и распространения информации (специализированные вычислительные центры, банки данных и базы знаний, информационные сети).

2) Создание новых материалов и технологий, роботизация промышленного производства, замена ручного труда машинным.

+3) Образование новой информационной инфраструктуры, которая позволяет совместное функционирование компьютеров и телефонов, спутников связи и иных новейших аппаратных средств.

+4) Конвергенция информационных сетей, связанная с объединением возможностей различных технических средств.

5) Появление новых рабочих мест, автоматизация производства, существенные сдвиги происходят в сфере занятости и трудоустройства.

+6) Создание процессами глобализации предпосылок для бурного роста информационных сетей и интернет-технологий. Сети формируются по зональному, функциональному и проблемному принципам.

+7) Образование глобальной инфраструктуры международного информационного обмена, ведущее к развитию системы информационных услуг.

8) **И**нформационные продукты превращаются в основной экономический ресурс наравне с оборотом товаров и услуг, становятся источником прибыли.

14. Что такое информационная культура?

+1) Информационная культура – это умение целенаправленно работать с информацией и использовать для ее получения, обработки и передачи компьютерную информационную технологию, современные технические средства и методы.

2) Информационная культура – это невозможность нанесения вреда свойствам объекта безопасности, обуславливаемым информацией и информационной инфраструктурой (защищенность от угроз).

3) Информационная культура – это способность каждого члена общества создавать получать, хранить и обрабатывать информацию не нанося ущерб другим членам общества, действовать в рамках юридических норм.

15. Дайте определение понятию «Информационная безопасность».

1) Информационная безопасность – это умение целенаправленно работать с информацией и использовать для ее получения, обработки и передачи компьютерную информационную технологию, современные технические средства и методы.

+2) Информационная безопасность – невозможность нанесения вреда свойствам объекта безопасности, обуславливаемым информацией и информационной инфраструктурой (защищенность от угроз).

3) Информационная безопасность – это защита от явных или непреднамеренных угроз при помощи специально разработанного программного обеспечения.

16. Перечислите основные задачи информационной безопасности.

(Внимание! Множественный ответ)

1) Обнаружение вредоносных программных продуктов, направленных для инфицирования компьютерной системы сетевым троллем.

+2) Своевременное выявление и устранение угроз безопасности и ресурсам, причин и условий, способствующих нанесению финансового, материального и морального ущерба его интересам.

+3) Создание механизма и условий оперативного реагирования на угрозы безопасности и проявлению негативных тенденций в функционировании предприятия.

4) Пресечение действий посторонних лиц по несанкционированному проникновению через локальную сеть в персональные данные.

+5) Эффективное пресечение посягательств на ресурсы и угроз персоналу на основе правовых, организационных и инженерно-технических мер и средств обеспечения безопасности.

+6) Создание условий для максимально возможного возмещения и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния последствий нарушения безопасности на достижение целей организации.

7) Обнаружение и изолирование подозрительных программных продуктов, пытающихся самостоятельно зарегистрироваться в сети интернет.

17. Перечислите виды информационных угроз.

(Внимание! Множественный ответ)

1) Угрозы техногенного характера.

+2) естественные угрозы (пожар, наводнение, и др.).

+3) человеческий фактор.

4) Угрозы структурного характера.

+5) угрозы, носящие случайный, неумышленный характер.

+6) угрозы, обусловленные умышленными**,** преднамеренными действиями людей.

7) Системные угрозы.

18. Что понимают под внутренними угрозами?

+1) Утечки информации и неавторизованный доступ.

2) Несанкционированный доступ к конфиденциальной информации.

3) Вредоносные программы, атаки хакеров, спам, фишинг.

19. Что понимают под внешними угрозами?

1) Взлом и проникновение в базы данных.

+2) Вредоносные программы, атаки хакеров, спам, фишинг.

3) Несанкционированный доступ к конфиденциальной информации.

20. Дайте определение компьютерного вируса.

1) Вирус – это полиморфные программы, каждая новая копия такого вредителя имеет иную цепочку кода, что затрудняет его детектирование и уничтожение.

2) Вирус – это текст, выполненный на особом языке, понятном машине. Он может выполняться непосредственно по тексту с помощью интерпретатора или транслироваться в особый вид с помощью компилятора.

+3) Вирус – исполняемый код, самостоятельно реплицирующий себя (либо видоизмененную вариацию). Это файловые/программные вирусы, размножающиеся путем внедрения в посторонний легитимный код.

21. На какие виды можно разделить вирусные программы?

(Внимание! Множественный ответ)

+1) Boot-вирусы – прописывают себя в загрузочный сектор накопителя информации.

+2) Макро/скрипт-вирусы – полиморфные вирусы, каждая новая копия такого вредителя имеет иную цепочку кода, что затрудняет его детектирование антивирусами.

3) Тролли – вирусы, провоцирующие преднамеренное искажение информации (чаще всего с переходом к другому смыслу), инфицирующие другие программы или (реже) выдающих себя за другие программы.

+4) Черви – саморазмножение в них реализовано по принципу деления, то есть распространение всевозможными способами и каналами.

+5) Трояны – программы, которые маскируются под доверенные приложения – на самом же деле они имеют враждебные функции. Троянские программы не могут распространяться сами по себе, и этим они отличаются от вирусов и червей

6) Roots – скрывающие свою сущность программы, которые находятся в нейтральном состоянии до определенного момента времени или команды.

22. Что представляет собой идентификация?

+1) Идентификация – это процедура распознавания субъекта по его идентификатору. В процессе регистрации субъект предъявляет системе свой идентификатор и она проверяет его наличие в своей базе данных.

2) Идентификация – это предоставление определённому лицу или группе лиц прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий.

3) Идентификация – это процедура использования социальной инженерии для получения доступа к конфиденциальной информации пользователей – логинам и паролям.

23. Что такое фишинговая атака?

1) Фишинговая атака – это комплекс, который включает компьютерное и коммуникационное оборудование, программное обеспечение, лингвистические средства, информационные ресурсы.

+2) Фишинг – вид интернет мошенничества с использованием социальной инженерии для получения доступа к конфиденциальной информации пользователей – логинам и паролям.

3) Фишинг – это разновидность вирусных программ, которые временно блокируют действия пользователя путем перехвата управления.

24. Дайте определение информационной системы.

1) Информационная система – это комплекс, который включает компьютерное и коммуникационное оборудование, программное обеспечение, лингвистические средства, информационные ресурсы.

+2) Информационная система – организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы.

3) Информационная система – инфраструктура, обеспечивающая реализацию информационных процессов сбора, обработки, накопления, хранения, поиска и распространения информации.

25. Что представляют собой информационные ресурсы?

1) Информационные ресурсы — это данные, организованные в виде набора записей определенной структуры и хранящиеся в файлах, где, помимо самих данных, содержится описание их структуры.

2) Информационные ресурсы — организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы.

+3) Информационные ресурсы — отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).

26. Что такое персональные данные?

+1) *Персональные данные (информация о гражданах)* — сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность.

2) *Персональные данные (информация о гражданах)* — отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).

3) *Персональные данные (информация о гражданах)* — цифровая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), несущая основные идентификационные маркеры личности.

27. Что представляет собой система обработки данных?

1) Система обработки данных – это совокупность программных продуктов направленная на максимально корректную обработку данных.

+2) Система обработки данных (СОД) – это комплекс взаимосвязанных методов и средств преобразования данных, необходимых пользователю.

3) Система обработки данных позволяет собирать, хранить и обрабатывать данные из различных источников, созданных на разных языках и платформах.

28. Что представляет собой автоматизированная информационная система?

1) Автоматизированная информационная система (АИС) – это совокупность информации на компьютере, собранная при случайных или преднамеренных воздействиях, которые могут принести определенный положительный эффект владельцу и пользователю этой информации.

2) Автоматизированная информационная система (АИС) – это инфраструктура, обеспечивающая реализацию информационных процессов сбора, обработки, накопления, хранения, поиска и распространения информации.

+3) Автоматизированная информационная система (АИС) – это комплекс, который включает компьютерное и коммуникационное оборудование, программное обеспечение, лингвистические средства, информационные ресурсы, а также системный персонал, обеспечивающий поддержку динамической информационной модели некоторой части реального мира для удовлетворения информационных потребностей пользователей и для принятия решений.

29. Назовите основные особенности структурных методов построения формализованной модели функционирования предприятия.

(Внимание! Множественный ответ.)

+1) расчленение сложной системы на части, представляемые как «черные ящики», каждый из них выполняет определенную функцию системы управления

2) последовательный переход от предыдущего состояния системы к последующему после завершения определенных действий.

+3) иерархическое упорядочение выделенных элементов системы с определением взаимосвязей между ними

+4) использование графического представления взаимосвязей элементов системы

5) применение иерархического подхода к решению задачи трассировки бизнес-процессов.

30. Чем отличается объектно-ориентированный подход к построению моделей информационных систем?

+1) Объектно-ориентированный подход к построению моделей информационных систем отличается большим уровнем абстракции и основывается на представлении системы в виде совокупности объектов, взаимодействующих между собой путем передачи определенных сообщений.

2) Объектно-ориентированный подход отличается тем, что происходит расчленение сложной системы на части, представляемые как «черные ящики», каждый из которых выполняет определенную функцию системы управления.

3) Отличие объектно-ориентированного подхода состоит в том, что выбираются несколько объектов и осуществляется последовательный переход от предыдущего состояния системы к последующему после завершения определенных действий.

31. Перечислите модели жизненного цикла программного обеспечения.

(Внимание! Множественный ответ)

1) Иерархическая модель – строгое следование процедуре в соответствии с установленной иерархией.

+2) Каскадная модель – последовательный переход на следующий этап после завершения предыдущего.

+3) Итерационная модель – с итерационными возвратами на предыдущие этапы после выполнения очередного этапа.

4) Глобальная модель – модель, имеющая структуру, включающую в себя другие модели в разных сочетаниях. Применятся при разработке сложных проектов, содержащих дробные объекты и/или объекты с внешними связями.

+5) Спиральная модель – прототипная модель, предполагающая постепенное расширение прототипа ИС.

6) Транспарентная модель – открытая модель, прозрачная для внесения новых процедур. Данное понятие применяется в качестве одной из разновидностей глобальной модели.

32. Что отображает спиральная модель жизненного цикла?

1) *Спиральная модель* жизненного цикла ИС отображает согласование проектных решений, получаемых при реализации отдельных задач. Данный подход к проектированию предполагает необходимость таких итерационных возвратов, когда проектные решения по отдельным задачам объединяются в общие системные решения, и при этом возникает потребность в пересмотре ранее сформулированных требований.

+2) *Спиральная модель* жизненного цикла ИС реально отображает разработку программного обеспечения; позволяет явно учитывать риск на каждом витке эволюции разработки; включает шаг системного подхода в

итерационную структуру разработки; использует моделирование для уменьшения риска и совершенствования программного изделия.

3) *Спиральная модель* жизненного цикла ИС отображает приемы планирования времени осуществления всех этапов проекта и упорядочения хода конструирования. Переход на следующий, иерархически нижний этап происходит только после полного завершения работ на текущем этапе.

33. Как выполняется криптографическое закрытие информации?

1) Криптографическое закрытие информации выполняется при помощи шифрования, где используются разные ключи, которые связаны между собой. Знание одного ключа не позволяет определить другой.

2) Криптографическое закрытие информации выполняется для сохранения исходной информации с использованием закрытого ключа и позволяет подтверждать целостность и неизменность этой информации, а также ее авторство путем применения открытого ключа.

+3) Криптографическое закрытие информации выполняется путем преобразования информации по специальному алгоритму с использованием процедур шифрования, в результате чего невозможно определить содержание данных, не зная ключа.

34. На чем основан принцип ассиметричного шифрования?

+1) Асимметричное шифрование основано на том, что для шифрования и дешифрования используются разные ключи, которые связаны между собой. Знание одного ключа не позволяет определить другой.

2) Принцип ассиметричного шифрования основан на преобразовании информации по специальному алгоритму с использованием процедур шифрования, в результате чего невозможно определить содержание данных, не зная ключа.

3) Принцип ассиметричного шифрования заключается в использовании разных ключей, которые связаны между собой. Знание одного ключа не позволяет определить другой.

35. Что представляет собой электронная цифровая подпись?

1) *Электронная цифровая подпись* – это способность системы управления реляционной базой данных уцелеть после аварии системы и воспроизвести выполненные транзакции.

+2) *Электронная цифровая подпись* – это последовательность символов, полученная в результате криптографического преобразования исходной информации с использованием закрытого ключа и позволяющая подтверждать целостность и неизменность этой информации, а также ее авторство путем применения открытого ключа.

3) *Электронная цифровая подпись* – это совокупность информации, собранная случайным образом под воздействием электронных меток, которые могут помогают владельцу этой информации сохранить ее в целостном виде.

36. Что представляет собой операция резервного копирования (backup)?

1) Операция резервного копирования (backup) – это способность системы управления реляционной базой данных (СУРБД – RDBMS) уцелеть после аварии системы и воспроизвести выполненные транзакции.

2) Операция резервного копирования (backup) – это процедура  восстановления данных из резервной копии путем копирования назад в базу данных.

+3) При выполнении операции резервного копирования (backup) данные копируются из базы данных и сохраняются в другом месте.

37. Что представляет собой воспроизведение (регенерация) данных?

+1) Воспроизведение (регенерация) (recovery) – это способность системы управления реляционной базой данных (СУРБД – RDBMS) уцелеть после аварии системы и воспроизвести выполненные транзакции.

2) Воспроизведение (регенерация) (recovery) – это процедура  восстановления данных из резервной копии путем копирования назад в базу данных.

3) Воспроизведение (регенерация) (recovery) – это выполнение операции резервного копирования, при которой данные копируются из базы данных и сохраняются в другом месте.

38. Что представляет собой операция восстановления (restore)?

1) Операция восстановления (restore) – это выполнение операции резервного копирования, при которой данные копируются из базы данных и сохраняются в другом месте.

+2) При выполнении операции восстановления (restore) данные из резервной копии копируются назад в базу данных.

3) Операция восстановления (restore) – это способность системы управления реляционной базой данных уцелеть после аварии системы и воспроизвести выполненные транзакции.

39. Что представляют собой сетевые фильтры?

1) Сетевые фильтры представляют собой устройства, благодаря которым при отключении внешнего питания устройства продолжают работать.

2) Сетевые фильтры представляют – это электрическое оборудование, которое позволяет сохранять работоспособность системы при полном отключении внешнего электропитания.

+3) Сетевые фильтры – наиболее дешевый способ защиты от сбоев электропитания с возможностью обесточивания одной кнопкой всех устройств, подключенных к нему (так и надо поступать, когда компьютер выключен).

40. Что представляют собой устройства бесперебойного питания?

+1) Такие устройства и выполняют работу сетевого фильтра, и имеют встроенный аккумулятор, благодаря которому при отключении внешнего электропитания подключенные к ИБП устройства продолжают работать.

2) Устройства бесперебойного питания – это наиболее дешевый способ защиты от сбоев электропитания с возможностью обесточивания одной кнопкой всех устройств, подключенных к нему (так и надо поступать, когда компьютер выключен).

3) Устройства бесперебойного питания представляют собой приборы для защиты устройств от длительных отключений электричества в сетях с переменным током, нестабильным напряжением и наличием серьезных помех.

4.4 Вопросы к экзамену или зачету

1. Дайте определение понятия «информация».
2. Что представляет собой информатизация?
3. Что представляет собой документированная информация (документ)?
4. Что представляют собой информационные ресурсы?
5. Что представляет собой информационная революция?
6. Когда произошла и с чем связана четвертая информационная революция?
7. Что представляет собой информационное обеспечение государственного управления?
8. Кто ввел понятие «информационное общество»?
9. Что понимают под термином «информационное общество»?
10. Перечислите основные признаки «информационного общества».
11. На какие области позволяет влиять «информационная экономика»?
12. Перечислите направления деятельности, связанные с информационным обслуживанием населения.
13. Перечислите этапы распространения новых информационных технологий.
14. Что такое информационная культура?
15. Дайте определение понятию «Информационная безопасность».
16. Перечислите основные задачи информационной безопасности.
17. Перечислите виды информационных угроз.
18. Что понимают под внутренними угрозами?
19. Что понимают под внешними угрозами?
20. Дайте определение компьютерного вируса.
21. На какие виды можно разделить вирусные программы?
22. Что представляет собой идентификация?
23. Что такое фишинговая атака?
24. Дайте определение информационной системы.
25. Что представляют собой информационные ресурсы?
26. Что такое персональные данные?
27. Что представляет собой система обработки данных?
28. Что представляет собой автоматизированная информационная система?

29. Назовите основные особенности структурных методов построения формализованной модели функционирования предприятия.
30. Чем отличается объектно-ориентированный подход к построению моделей информационных систем?
31. Перечислите модели жизненного цикла программного обеспечения.
32. Что отражает спиральная модель жизненного цикла?
33. Как выполняется криптографическое закрытие информации?
34. На чем основан принцип ассиметричного шифрования?
35. Что представляет собой электронная цифровая подпись?
36. Что представляет собой операция резервного копирования (backup)?
37. Что представляет собой воспроизведение (регенерация) данных?
38. Что представляет собой операция восстановления (restore)?
39. Что представляют собой сетевые фильтры?
40. Что представляют собой устройства бесперебойного питания?

4.5 Темы рефератов

1. Информация – фактор существования и развития общества. Основные формы проявления информации, её свойства как объекта безопасности.
2. Понятие безопасности и её составляющие. Безопасность информации.
3. Обеспечение информационной безопасности: содержание и структура понятия.
4. Национальные интересы в информационной сфере.
5. Источники и содержание угроз в информационной сфере.
6. Соотношение понятий «информационная безопасность» и «национальная безопасность»
7. Понятие национальной безопасности. Интересы и угрозы в области национальной безопасности.
8. Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание.
9. Система обеспечения информационной безопасности.
10. Понятие информационной войны. Проблемы информационной войны.
11. Информационное оружие и его классификация.
12. Цели информационной войны, её составные части и средства её ведения. Объекты воздействия в информационной войне.
13. Уровни ведения информационной войны. Информационные операции. Психологические операции. Оперативная маскировка. Радиоэлектронная борьба. Воздействие на сети.
14. Основные положения государственной информационной политики. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности.
15. Виды защищаемой информации в сфере государственного и муниципального управления.
16. Обеспечение информационной безопасности организации.
17. Управление и защита информации в информационно-телекоммуникационных сетях.
18. Характеристика эффективных стандартов по безопасности. Требования к полноте эффективных стандартов по безопасности.
19. Риск работы на персональном компьютере. Планирование безопасной работы на персональном компьютере.
20. Стандарты предприятия по использованию персональных компьютеров. Практические меры безопасности для персональных компьютеров.