**Тестовые задания по учебнику Н.Д.Угриновича**

**Глава 1. Компьютер как средство автоматизации информационных процессов.**

**§ 1.4.1 Защита с использованием паролей**

**Задание # 1**

*Вопрос:*

Для защиты от несанкционированного доступа к программам и данным, хранящимся на компьютере, используются

*Выберите один из 4 вариантов ответа:*

1) пароли

2) анкеты

3) коды

4) ярлыки

**§ 1.4.2 Биометрические системы защиты**

**Задание # 2**

*Вопрос:*

От несанкционированного доступа может быть защищён:

*Выберите несколько из 4 вариантов ответа:*

1) каждый диск

2) папка

3) файл

4) ярлык

**Задание # 3**

*Вопрос:*

К биометрическим системам защиты информации относятся системы идентификации по:

*Выберите несколько из 9 вариантов ответа:*

1) отпечаткам пальцев

2) характеристикам речи

3) радужной оболочке глаза

4) изображению лица

5) геометрии ладони руки

6) росту

7) весу

8) цвету глаз

9) цвету волос

**§ 1.5 Физическая защита данных на дисках**

**Задание # 4**

*Вопрос:*

Какие существуют массивы дисков RAID?

*Выберите несколько из 4 вариантов ответа:*

1) RAID 0

2) RAID 1

3) RAID 10

4) RAID 20

**Задание # 5**

*Вопрос:*

Найди соответствие.

*Укажите соответствие для всех 2 вариантов ответа:*

1) Для создания массива этого уровня понадобится как минимум два диска одинакового размера. Запись осуществляется по принципу чередования: данные делятся на порции одинакового размера (А1, А2, А3 и т.д.), и поочерёдно распределяются по всем дискам, входящим в массив.

2) Массивы этого уровня построены по принципу зеркалирования, при котором все порции данных (А1, А2, А3 и т.д.), записанные на одном диске, дублируются на другом.

\_\_ RAID 0

\_\_ RAID 1

**§ 1.6.1 Вредоносные и антивирусные программы**

**Задание # 6**

*Вопрос:*

Выберите типы вредоносных программ:

*Выберите несколько из 6 вариантов ответа:*

1) Вирусы, черви, троянские и хакерские программы

2) Шпионское, рекламное программное обеспечение

3) Потенциально опасное программное обеспечение

4) Операционная система Linux

5) Операционная система Windows

6) Microsoft Office

**Задание # 7**

*Вопрос:*

Найди соответствие.

*Укажите соответствие для всех 2 вариантов ответа:*

1) сигнатуры. Сигнатура - это некоторая постоянная последовательность программного кода, специфичная для конкретной вредоносной программы.

2) алгоритмы эвристического сканирования, т.е.анализа последовательности команд в проверяемом объекте.

\_\_ Для поиска известных вредоносных программ используются

\_\_ Для поиска новых вирусов используются

**Задание # 8**

*Вопрос:*

Найди соответствие.

*Укажите соответствие для всех 2 вариантов ответа:*

1) автоматически при старте операционной системы и работает в качестве фонового системного процессора, проверяя на вредоносность совершаемые другими программами действия. Основная задача состоит в обеспечении максимальной защиты от вредоносных программ при минимальном замедлении работы компьютера.

2) по заранее выбранному расписанию или в произвольный момент пользователем. Производит поиск вредоносных программ в оперативной памяти, а также на жестких и сетевых дисках компьютера.

\_\_ Антивирусный монитор запускается

\_\_ Антивирусный сканер запускается

**§ 1.6.2 Компьютерные вирусы и защита от них**

**Задание # 9**

*Вопрос:*

Компьютерные вирусы -

*Выберите один из 5 вариантов ответа:*

1) являются вредоносными программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.

2) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Их активизация может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.

3) вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.

4) это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров.

5) программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.

**Задание # 10**

*Вопрос:*

По "среде обитания" вирусы можно разделить на:

*Выберите несколько из 6 вариантов ответа:*

1) загрузочные

2) файловые

3) макровирусы

4) очень опасные

5) не опасные

6) опасные

**Задание # 11**

*Вопрос:*

Найди соответствие.

*Укажите соответствие для всех 3 вариантов ответа:*

1) заражают загрузочный сектор гибкого или жёсткого диска.

2) эти вирусы различными способами внедряются в исполнимые файлы и обычно активизируются при их запуске.

3) существуют для интегрированного офисного приложения Microsoft Office.

\_\_ загрузочные вирусы

\_\_ файловые вирусы

\_\_ макровирусы

**§ 1.6.3 Сетевые черви и защита от них**

**Задание # 12**

*Вопрос:*

Сетевые черви -

*Выберите один из 5 вариантов ответа:*

1) являются вредоносными программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.

2) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Их активизация может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.

3) вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.

4) это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров.

5) программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.

**Задание # 13**

*Вопрос:*

Сетевые черви бывают:

*Выберите несколько из 4 вариантов ответа:*

1) Web-черви

2) почтовые черви

3) черви операционной системы

4) черви MS Office

**Задание # 14**

*Вопрос:*

Найди соответствие.

*Укажите соответствие для всех 2 вариантов ответа:*

1) Профилактическая защита от таких червей состоит в том, что в браузере можно запретить получение активных элементов на локальный компьютер.

2) Профилактическая защита от таких червей состоит в том, что не рекомендуется открывать вложенные в сообщения файлы, полученные от сомнительных источников. А также рекомендуется своевременно скачивать из Интернета и устанавливать обновления системы безопасности операционной системы и приложений.

\_\_ Web-черви

\_\_ почтовые черви

**Задание # 15**

*Вопрос:*

Наиболее эффективны от Web-червей, Web-антивирусные программы, которые включают:

*Выберите несколько из 3 вариантов ответа:*

1) межсетевой экран

2) модуль проверки скриптов

3) антивирусный сканер

**Задание # 16**

*Вопрос:*

Межсетевой экран (брандмауэр) -

*Выберите один из 5 вариантов ответа:*

1) являются вредоносными программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.

2) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Их активизация может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.

3) вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.

4) это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров.

5) программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.

**§ 1.6.4 Троянские программы и защита от них**

**Задание # 17**

*Вопрос:*

Троянская программа, троянец -

*Выберите один из 5 вариантов ответа:*

1) являются вредоносными программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.

2) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Их активизация может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.

3) вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.

4) это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров.

5) программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.

**Задание # 18**

*Вопрос:*

Троянские программы бывают:

*Выберите несколько из 4 вариантов ответа:*

1) утилиты удалённого администрирования

2) программы - шпионы

3) рекламные программы

4) программы удаления данных на локальном компьютере

**Задание # 19**

*Вопрос:*

Найди соответствие.

*Укажите соответствие для всех 3 вариантов ответа:*

1) троянские программы данного типа являются одним из самых опасных видов вредоносного программного обеспечения, поскольку в них заложена возможность самых разнообразных злоумышленных действий, в том числе они могут быть использованы для обнаружения и передачи кофиденциальной информации.

2) троянские программы этого типа часто используются для кражи информации пользователей различных систем онлайновых платежей и банковских систем.

3) эти программы встраивают рекламу в основную полезную программу и могут выполнять функцию троянских программ. Эти программы могут скрытно собирать различную информацию о пользователе компьютера и затем отправлять её злоумышленнику.

\_\_ Троянские утилиты удалённого администрирования

\_\_ Троянские программы - шпионы

\_\_ Рекламные программы

**§ 1.6.5 Хакерские утилиты и защита от них**

**Задание # 20**

*Вопрос:*

Найди соответствие.

*Укажите соответствие для всех 2 вариантов ответа:*

1) реализуют атаку с одного компьютера с ведома пользователя. Эти программы обычно наносят ущерб удалённым компьютерам и сетям, не нарушая работоспособности заражённого компьютера.

2) реализуют распределённые атаки с разных компьютеров, причём без ведома пользователей заражённых компьютеров.

\_\_ DoS - программы

\_\_ DDos - программы

**Задание # 21**

*Вопрос:*

Руткит -

*Выберите один из 5 вариантов ответа:*

1) являются вредоносными программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.

2) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Их активизация может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.

3) вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.

4) это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров.

5) программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.

**Задание # 22**

*Вопрос:*

Межсетевой экран позволяет:

*Выберите несколько из 5 вариантов ответа:*

1) блокировать хакерские DoS - атаки, не пропуская на защищаемый компьютер сетевые пакеты с определённых серверов

2) не допускать проникновение на защищаемый компьютер сетевых червей

3) препятствовать троянским программам отправлять конфиденциальную информацию о пользователе и компьютере

4) видеть действия котрые выполняет пользователь на другом компьютере

5) использовать принтер подключённый к другому компьютеру

**Ответы:**

1) Верный ответ (1 б.): 1;

2) Верные ответы (1 б.): 1; 2; 3;

3) Верные ответы (1 б.): 1; 2; 3; 4; 5;

4) Верные ответы (1 б.): 1; 2;

5) Верные ответы (1 б.):

 1; 2;

6) Верные ответы (1 б.): 1; 2; 3;

7) Верные ответы (1 б.):

 1; 2;

8) Верные ответы (1 б.):

 1; 2;

9) Верный ответ (1 б.): 1;

10) Верные ответы (1 б.): 1; 2; 3;

11) Верные ответы (1 б.):

 1; 2; 3;

12) Верный ответ (1 б.): 2;

13) Верные ответы (1 б.): 1; 2;

14) Верные ответы (1 б.):

 1; 2;

15) Верные ответы (1 б.): 1; 2;

16) Верный ответ (1 б.): 4;

17) Верный ответ (1 б.): 3;

18) Верные ответы (1 б.): 1; 2; 3;

19) Верные ответы (1 б.):

 1; 2; 3;

20) Верные ответы (1 б.):

 1; 2;

21) Верный ответ (1 б.): 5;

22) Верные ответы (1 б.): 1; 2; 3;

Конец