

Министерство науки и высшего образования Российской Федерации  
ФГБОУ ВО «Удмуртский государственный университет»  
Институт экономики и управления  
Кафедра государственной службы и управления персоналом

**А.А. МУХИН**

## **ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

Сборник контрольных заданий (тестов)



Ижевск  
2023

УДК 342.9(075.8)  
ББК 67.401я73  
М925

*Рекомендовано к изданию учебно-методическим советом УдГУ*

**Рецензент:** канд. экон. наук, доцент, ин-т экономики и управления ФГБОУ ВО «Удмуртский государственный университет» А.Н. Суетин.

**Мухин А.А.**

М925 Информационная безопасность : сб. контрольных заданий (тестов)  
[Электрон. ресурс] – Ижевск : Удмуртский университет, 2023. – 47 с.

Предназначено для студентов юридических вузов, обучающихся по направлениям «Юриспруденция», «Юриспруденция (бакалавр)», «Правоохранительная деятельность», «Судебная и прокурорская деятельность», «Правовое обеспечение национальной безопасности», «Государственное и муниципальное управление», а также для аспирантов юридических вузов, практических работников.

Соответствует актуальным требованиям Федерального государственного образовательного стандарта высшего образования.

Решение задач преследует цель закрепить теоретические знания, полученные на теоретических занятиях.

УДК 342.9(075.8)  
ББК 67.401я73

© А.А. Мухин, 2023  
© ФГБОУ ВО «Удмуртский  
государственный университет», 2023

## Оглавление

Предисловие.....	4
Тема 1. Эволюция каналов передачи информации.....	6
Тема 2. Понятия и определения в области информационной безопасности.....	8
Тема 3. Информационные угрозы и способы защиты от них.....	10
Тема 4. Доктрина информационной безопасности ..... Российской Федерации .....	13
Тема 5. Защита информации .....	14
Тема 6. Законодательный уровень защиты информации .....	16
Тема 7. Процедурный уровень обеспечения информационной безопасности ...	18
Тема 8. Компьютерные вирусы и антивирусные программы.....	20
Тема 9. Методы и технологии борьбы с компьютерными вирусами .....	21
Тема 10. Криптография.....	23
Тема 11. Биометрия .....	25
Тема 12. Индивидуальная и государственная защита информации .....	27
Тема 13. Информационная война .....	29
Тема 14. Информационный терроризм .....	30
Тема 15. «Особенности управления информации в городах» .....	32
Тема 16. Особенности обеспечения информационной безопасности Российской Федерации в различных сферах общественной жизни .....	34
Тема 17. Информационная экономика .....	36
Тема 18. Глобальная информатизация общества .....	37
Тема 19. Воздействие средств массовой информации .....	39
Тема 20. Реклама как источник информационной опасности .....	40
Тема 21. Ложь как источник информационной опасности .....	41
Тема 22. Информационные образовательные технологии XXI века .....	42
Тема 23. Информационная экология.....	43
Тема 24. Географические информационные системы .....	45
Тема 25. Актуальные вопросы обеспечения безопасности..... и развития детей в информационном пространстве .....	47

## Предисловие

Практикум по выполнению практических заданий используется при изучении дисциплины «Информационная безопасность».

В практикуме рассмотрены следующие темы: эволюция каналов передачи информации, понятия и определения в области информационной безопасности, информационные угрозы и способы защиты от них, доктрина информационной безопасности Российской Федерации, защита информации, законодательный уровень защиты информации, процедурный уровень обеспечения информационной безопасности, компьютерные вирусы и антивирусные программы, методы и технологии борьбы с компьютерными вирусами, криптография, биометрия, индивидуальная и государственная защита информации, информационная война, информационный терроризм, особенности управления информацией в городах, особенности обеспечения информационной безопасности, Российской Федерации в различных сферах общественной жизни, информационная экономика, глобальная информатизация общества, воздействие средств массовой информации, реклама как источник информационной опасности, ложь как источник информационной опасности, информационные образовательные технологии XXI века, информационная экология, географические информационные системы, актуальные вопросы обеспечения безопасности и развития детей в информационном пространстве.

Основная цель практикума: формирование у студентов системы теоретических знаний и практических умений, связанных с их профессиональной компетентностью, ознакомление студентов с тенденцией развития информационной безопасности, с моделями возможных угроз, терминологией и основными понятиями теории безопасности информации, а также с нормативными документами РФ по данному вопросу.

**Цели преподавания курса:** изучение роли, места и универсальный характер функции обеспечения безопасности в жизнедеятельности общества.

### **Задачи освоения дисциплины:**

- оказание помощи физическим и юридическим лицам в защите их прав и законных интересов;
- обеспечение законности и правопорядка, экономической безопасности общества, государства, личности и иных субъектов экономической деятельности;
- проведение прикладных научных исследований в соответствии с профилем своей профессиональной деятельности.

В результате освоения дисциплины обучающийся должен:

**Знать:**

- общие положения информационной безопасности;
- вредоносные программы и защита от них;
- информационную безопасность в компьютерных сетях;
- методы принятия решений в разработке системы информационной безопасности;
- информационную безопасность в компьютерных сетях;
- информационное законодательство;
- информационные правоотношения;
- правовые режимы информации;
- правовое регулирование отношений в сфере охраны государственной тайны;
- ответственность за правонарушения в информационной сфере.

**Уметь:**

- применять стандарты информационной безопасности;
- применять стандарты информационной безопасности распределенных систем.
- классифицировать угрозы информационной безопасности.
- анализировать угрозы информационной безопасности.
- применять антивирусные программы.
- классифицировать удаленные угрозы в вычислительных сетях.
- анализировать типовые удаленные атаки и давать их характеристику.
- принимать решения в разработке системы информационной безопасности.
- применять нормативные правовые акты, регулирующие отношения в информационной сфере.
- называть субъекты информационных правоотношений и объекты информационных правоотношений.
- применять режим свободного доступа, режим ограниченного доступа.
- выстраивать доступ к государственной тайне.
- применять государственную политику информационной безопасности и организационную основу системы ее обеспечения.
- применять юридическую ответственность за нарушение законодательства в информационной сфере.

**Владеть:**

- обеспечением законности и правопорядка, экономической безопасности общества, государства, личности и иных субъектов экономической деятельности;
- оказание помощи физическим и юридическим лицам в защите их прав и законных интересов.

## Тема 1. Эволюция каналов передачи информации

**1. Информационная безопасность может быть представлена на нескольких уровнях. Распределите особенности по уровням:**

*Соедините элементы попарно*

1. уровень локальной среды
2. уровень личности
3. уровень общества

а. характеристика национальной безопасности, где присутствует информационная безопасность, обеспечивающая качество жизни и здоровье людей
б. способность сохранять сопротивляемость к деструктивным внутренним и внешним воздействиям среды
с. место, где работает, живет человек, его семья, окружение друзей

1 – с

2 – б

3 – а

**2. Эволюция каналов передачи информации сопряжена:**

1. с эволюцией способов передачи информации
2. с языковым разнообразием
3. с развитием структуры общества
4. с географической удаленностью

**3. Какими особенностями обладает область информационных и телекоммуникационных технологий?**

1. сегменты информатики соединены для обеспечения услуг по обработке речи, текста, изображения, данных и видеоинформации
2. неуклонный рост соотношения между мощностью вычислительной техники и стоимостью электронно-вычислительных операций
3. беспроводные системы открыли возможность для предоставления услуг с высокими капитальными затратами
4. цифровые технологии позволили интегрировать телекоммуникационную и вычислительную отрасли
5. расширение цифровых систем без быстрого снижения издержек по передаче информации по различным каналам связи

**4. Расположите способы распространения информации в порядке появления (с раннего).**

*Расставьте в правильном порядке*

1. создание первой электронно-вычислительной машины
2. появление письменности
3. изобретение книгопечатания

4. изобретение важнейших средств связи (телеграф, телефон, радио)
5. изобретение первого микропроцессора

Ответ: 4, 1, 2, 3, 5

**5. Укажите состояния информационной безопасности личности:**

1. стабильная информационная безопасность
2. отсутствие информационной безопасности
3. незащищенность в конкретной ситуации
4. устойчивая информационная безопасность
5. защищенность в конкретной ситуации

## Тема 2. Понятия и определения в области информационной безопасности

### 1. Объем информации измеряют:

1. объемом мозга
2. длиной магнитной ленты с видео- и аудиозаписью
3. в страницах текста
4. уровнем IQ
5. количеством знаний у человека
6. в байтах / битах

### 2. Укажите лишний критерий информационной безопасности:

1. конфиденциальность
2. целостность
3. доступность
4. истинность

### 3. С середины XX в. понятие «информация» становится общенаучным и трактуется как:

1. обмен сведениями между человеком и автоматом
2. обмен сведениями между автоматом и автоматом
3. обмен сведениями между человеком и инопланетным существом
4. обмен сигналами и передача признаков от организма к организму
5. обмен сведениями между людьми
6. обмен сигналами между объектами живой и неживой природы

### 4. Распределите характеристики внутренней и внешней информации

*Переместите ответы в соответствующие группы ниже (используются все ответы)*

1. Внешняя информация
2. Внутренняя информация

a. Использование санкционировано только для внутреннего потребления
b. Содержится в массивах данных, документах и файлах, не предназначенных для передачи во внешнюю среду
c. Создается, потребляется, распространяется самой системой
d. Циркулирует в каналах обмена с иными системами
e. Основной продукт деятельности системы

1 – d, e

2 – a, b, c



**5. Для обозначения ценности конфиденциальной коммерческой информации используют три категории. Соотнесите категорию с описанием:**

*Соедините элементы попарно*

1. «коммерческая тайна – строго конфиденциально»
2. «коммерческая тайна – конфиденциально»
3.«коммерческая тайна»

а. доступность информации только определенному кругу лиц
б. производственная, научно-техническая, управленческая, финансовая или иная документированная информация, используемая для достижения коммерческих целей (получения прибыли, предотвращения ущерба)
с. особый контроль над доступом к информации

**1 – с**

**2 – а**

**3 – б**

### Тема 3. Информационные угрозы и способы защиты от них

1. Распределите виды угроз информационной безопасности по категориям.

1. Информационные:
2. Физико-технические:
3. Программно-математические:
4. Организационные:
  - a. Разрушение информационных файлов или системы доступа
  - b. Ошибки персонала систем
  - c. Хищения
  - d. Манипулятивные воздействия на личность
  - e. Психологические
  - f. Подделка и изменение данных
  - g. Кража секретов: патентов, стратегических планов, паролей
  - h. Видоизменение информации

1 – d, e

2 – b

3 – a, f, h

4 – c, g

2. При организации систем безопасности необходимо учитывать основные группы методов при несанкционированном доступе. Соотнесите метод с описанием.

*Соедините элементы попарно*

<b>Имитация</b>	Подмена информации в процессе ее ввода или вывода; данные фальсифицируются за счет замены истинных документов на фальшивые
<b>Сканирование</b>	Анализ всей доступной информации; просмотр мусорных корзин, оставленных дискет, анализ «стертых» файлов
<b>«Троянский конь»</b>	Подмена известной программы аналогом с дополнительными скрытыми функциями, которые можно использовать независимо от воли владельца программы
<b>Суперотключение</b>	Специфическая группа методов, основанных на вход в систему в сбойных ситуациях (создана по образцу программ для обхода системных мер защиты и доступа к компьютеру и его информации при аварийных ситуациях)
<b>«Технология салями»</b>	Несанкционированные доступы, совершаемые понемногу, небольшими частями, настолько маленькими, что они незаметны, со временем приводящие к изменениям базовой компьютерной программы
<b>«Люк»</b>	Использование скрытого программного или аппаратного механизма, позволяющего обойти методы защиты в системе и войти в нее; этот механизм активируется

некоторым неочевидным образом, неожиданно запуская авторизованную программу
---

**3. Несанкционированный доступ к информационным системам может быть осуществлен по \_\_\_\_\_ каналам, к которым относятся терминал пользователей, средства отображения и документирования информации, загрузка программного обеспечения, технологический пульт и органы управления.**

1. Контролируемым
2. Неконтролируемым
3. Внешним
4. Внутренним

**4. Идентификация и классификация возможных угроз повышает эффективность защиты. Своевременно обнаружить угрозу несанкционированного доступа помогают:**

1. ранжирование угроз по вероятности осуществления
2. отсутствие перечня потенциальных посягателей на информацию
3. применение технических средств обнаружения посягательства с характеристиками, позволяющими минимизировать время обнаружения несанкционированного доступа
4. мониторинг состояния уязвимых направлений деятельности субъекта или объекта
5. применение физической охраны для обнаружения посягательства на информацию

**5. Соедините последствия несанкционированного доступа к данным информационных систем с определениями.**

*Соедините элементы попарно*

Утрата	Стирание, искажение, уничтожение или хищение (безвозвратная потеря) информации, находящейся в процессе обработки или хранения в информационной системе
Искажение	Результат обработки данных не сертифицированными программами, которые вносят систематические погрешности в позиционные данные
Взлом системы	Модификация программного обеспечения, обеспечивающая его работу без ключей защиты, что дает возможность простого анализа данных информационной системы, имеющих специальные форматы, не читаемые другими программными средствами
Модификация программ	Изменение свойств программ при внешней корректности их работы
Утечка	Несанкционированное ознакомление постороннего лица с секретной информацией

Модификация данных	Изменение информации на ложную, но корректную по форме и содержанию; опасность заключается в возможности организации утечки секретной или (и) передачи ложной информации
--------------------	--

## **Тема 4. Доктрина информационной безопасности Российской Федерации**

**1. Доктрина информационной безопасности РФ рассматривает всю работу в интересах концепции \_\_\_\_\_ безопасности Российской Федерации**

1. Международной
2. Общественной
3. Национальной
4. Индивидуальной

**2. А) Первая составляющая национальных интересов в информационной сфере включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения и пользования информацией традиций патриотизма и гуманизма, культурного и научного потенциала страны.**

**Б) Третья составляющая национальных интересов в информационной сфере включает в себя развитие информационных технологий, средств информатизации, телекоммуникации и связи государственной политики Российской Федерации**

1. оба утверждения верны
2. верно только утверждение А
3. верно только утверждение Б
4. оба утверждения неверны

**3. Вторая составляющая национальных интересов в информационной сфере включает в себя \_\_\_\_\_ государственной политики Российской Федерации**

1. Информационное обеспечение
2. Безграничный доступ
3. Защиту
4. Распространение

**4. Четвертая составляющая национальных интересов в информационной сфере включает в себя \_\_\_\_\_ информационных ресурсов от несанкционированного доступа**

Ответ: Защиту

**5. Что из нижеперечисленного не выделяется в Доктрине как национальные интересы Российской Федерации в информационной сфере?**

1. сбор, хранение, использование и распространение информации о частной жизни лица
2. информационное обеспечение государственной политики Российской Федерации
3. соблюдение конституционных прав и свобод человека и гражданина в области получения и пользования информацией
4. защита информационных ресурсов от несанкционированного доступа
5. развитие современных информационных технологий

## Тема 5. Защита информации

1. Перспективным методом обнаружения сетевых атак следует считать использование \_\_\_\_\_, которая имеет механизм самообучения

Ответ: Нейросети

2. В какой период возникла необходимость создания систем распределенной обработки информации и систем коллективного пользования?

1. в середине 1980-х – начале 1990-х гг.
2. в конце 1990-х гг.
3. в 1970-е гг.
4. в начале 1980-х гг.

3. В среде информационных систем и информационных технологий информационная защита должна обеспечиваться на шести уровнях. Сопоставьте уровень с соответствующим описанием:

1. Физический	a. в целях повышения сохранности результатов обработки результатов предыдущего шага, обработки данных должны сохраняться до выполнения текущего шага (система отката)
2. Структурный	b. пользователь не имеет доступа к носителям информации
3. Алгоритмический	c. заложены принципы защиты информации и программного обеспечения
4. Аппаратный	d. обеспечены внутренняя непротиворечивость алгоритмов обработки и возможность контроля внешнего несанкционированного доступа
5. Концептуальный	e. специальное системное программное обеспечение должно контролировать состояние векторов прерываний для исключения доступа к процессу обработки к данным со стороны программ-шпионов
6. Программный	f. система ключей исключает доступ к программному обеспечению

- 1 – b
- 2 – d
- 3 – a
- 4 – f
- 5 – c
- 6 – e

**4. Защита информации от несанкционированного использования может быть \_\_\_\_\_ (режим открытости, доступности для всех заинтересованных лиц) и \_\_\_\_\_ (режимы секретности и разграничения доступа)**

1. Пассивной и активной
2. Активной и пассивной
3. Простой и сложной
4. Сложной и простой

**5. Различные системы контроля доступа можно разделить на классы в соответствии с тем, что человек должен предъявлять системе. Укажите типы предъявляемой информации:**

1. зачитывание конституционных прав и свобод человека и гражданина в области получения и пользования информацией

2. различного рода шифры, набираемые человеком (например, PIN-коды, криптографические коды)

3. использование звукового кодирования (Азбука Морзе)

4. шифры, предъявляемые при помощи физических носителей информации (пластиковые карты с магнитной полосой, электронные таблетки «touch memo», электронные token-устройства, proximity-карты)

5. биометрического класс, принципиально отличающегося тем, что идентификации подвергается собственно личность человека – его индивидуальные характеристики (рисунок папиллярного узора, радужная оболочка глаза)

## Тема 6. Законодательный уровень защиты информации

### 1. Заполните пропуски в выписке из Уголовного кодекса Российской Федерации (редакция от 14 марта 2002 года):

Глава 28 «Преступления в сфере компьютерной информации» содержит статьи:

- статья 272. Неправомерный доступ к информации с посягательствами на \_\_\_\_\_;
- статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети с нарушениями доступности, \_\_\_\_\_ информации.

Ответ: конфиденциальность; целостности.

### 2. Укажите верное утверждение.

1. Закрытый ключ электронной цифровой подписи – уникальная последовательность символов, известная владельцу сертификата ключа подписи.

2. Открытый ключ электронной цифровой подписи – уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступной ограниченному числу пользователей информационной системы.

- 1) оба утверждения верны
- 2) верно только утверждение 1
- 3) верно только утверждение 2
- 4) оба утверждения неверны

### 3. Соотнесите основные понятия закона «Об информации, информатизации и защите информации» (20 февраля 1995) с определениями.

документированная информация (документ) (1)	документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах) (6)
информация (2)	сбор, обработка, накопление, хранение, поиск и распространение информации (4)
пользователь (потребитель) информации (3)	сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность (5)
информационные процессы (4)	организационно упорядоченная совокупность документов (массивов документов) и информационных технологий (7)
информация о гражданах (персональные данные) (5)	зафиксированная на материальном носителе, информация с реквизитами, позволяющими ее идентифицировать (1)



информационные ресурсы (6)	субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею (3)
информационная система (7)	сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления (2)

**4. Какие цели защиты выделяются в законе «Об информации, информатизации и защите информации» (20 февраля 1995)?**

1) информационное обеспечение государственной политики Российской Федерации

2) предотвращение утечки, хищения, утраты, искажения, подделки информации

3) предотвращение угроз безопасности личности, общества, государства

4) защита информационных ресурсов от несанкционированного доступа

5) предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации

**5. Для защиты интересов субъектов информационных отношений необходимо сочетать меры следующих уровней. Сопоставьте уровни с их описанием:**

процедурный (1)	меры безопасности, ориентированные на людей (1)
программно-технический (2)	основной закон Российской Федерации – Конституция (04.07.2020 г.) (4)
административный (3)	приказы и другие действия руководства организаций, связанные с защищаемыми информационными системами (3)
законодательный (4)	меры безопасности в техническом и программном обеспечении (2)

**6. Вставьте пропущенное словосочетание.**

Статья 138 УК РФ, защищая конфиденциальность персональных данных, предусматривает наказание за нарушение \_\_\_\_\_, телефонных переговоров, иных сообщений.

Ответ: Тайны переписки

## Тема 7. Процедурный уровень обеспечения информационной безопасности

### 1. Избыточность обеспечения информационной безопасности выражается:

- 1) поддержкой пользователей и программного обеспечения
- 2) представлением информации на бумаге и в файлах
- 3) доступом к данным ограниченного числа лиц
- 4) мерами резервного копирования
- 5) хранением копий в нескольких местах

### 2. Расположите нижеперечисленные этапы процесса планирования восстановительных работ в правильном порядке:

- 1) проверка стратегии ШЕСТОЕ
- 2) определение перечня возможных аварий ТРЕТЬЕ
- 3) идентификация ресурсов, необходимых для выполнения критически важных функций ВТОРОЕ
- 4) разработка стратегии восстановительных работ ЧЕТВЁРТОЕ
- 5) подготовка к реализации выбранной стратегии ПЯТОЕ
- 6) выявление критически важных функций организации, установление приоритетов ПЕРВОЕ

### 3. Вставьте пропущенные слова на месте пропусков.

Стратегию восстановительных работ целесообразно провести с анализа \_\_\_\_\_, которым подвергаются критичные функции, и попытаться выбрать наиболее \_\_\_\_\_ решение.

Ответ: рисков; экономичное.

### 4. Сопоставьте классы мер процедурного уровня обеспечения информационной безопасности с соответствующими описаниями.

планирование восстановительных работ (1)	избежать ошибки системных администраторов и пользователей — максимально автоматизировать работу (2)
поддержание работоспособности (2)	локализация инцидента и уменьшение наносимого вреда; выявление нарушителя; предупреждение повторных нарушений (5)
физическая защита (3)	выявление критически важных функций организации, установление приоритетов; идентификация ресурсов для выполнения (1)
управление персоналом (4)	составление описания должности, разделение обязанностей, минимизация привилегий, прием сотрудника на работу

	(4)
реагирование на нарушения режима безопасности (5)	меры для защиты зданий и прилегающей территории, поддерживающей инфраструктуры, вычислительной техники, носителей данных (3)

**5. Выделите направления повседневной деятельности обеспечения информационной безопасности:**

- 1) распространение пользовательских данных
- 2) поддержка пользователей и программного обеспечения
- 3) управление носителями
- 4) один постоянный пароль системного администратора
- 5) резервное копирование
- 6) регламентные работы, документирование

## Тема 8. Компьютерные вирусы и антивирусные программы

### 1. Вставьте пропущенное слово.

Недооценка защиты от компьютерных вирусов и разрушающих программных средств может иметь серьезные последствия для \_\_\_\_\_ пользователей.

Ответ: информации.

### 2. По сложности, степени совершенства и особенностям маскировки алгоритмов вирусы, изменяющие среду обитания, подразделяются:

- 1) на полиморфные вирусы, имеющие совпадения кодов
- 2) на студенческие вирусы, имеющие низкую квалификацию
- 3) на вирусы-«спутники» и вирусы-«черви»
- 4) на «стелс»-вирусы, противодействующие антивирусным средствам
- 5) на полиморфные вирусы, не имеющие совпадений кодов

### 3. Распределите виды компьютерных вирусов по способу классификации:

сетевые, файловые, загрузочные и комбинированные (1)	алгоритм функционирования (3)
резидентные и нерезидентные (2)	способ заражения (2)
не изменяющие файлы и секторы при распространении; изменяющие среду обитания при распространении (3)	степень опасности (4)
Безвредные (4)	среда обитания (1)

### 4. Укажите функциональный модуль, которого нет в вирусе:

- 1) модуль самоуничтожения
- 2) модуль выполнения вредительских действий
- 3) модуль заражения (распространения)
- 4) модуль маскирования

### 5. Укажите верное утверждение.

1. Компьютерные вирусы – это небольшие исполняемые или интерпретируемые программы, обладающие свойством распространения и самовоспроизведения и неспособные модифицироваться в процессе распространения.

2. В каталог вирусов помещаются следующие сведения о стандартных свойствах вируса: имя, длина, заражаемые файлы, место внедрения в файл, метод заражения, способ внедрения в ОС для резидентных вирусов, вызываемые эффекты, наличие (отсутствие) деструктивной функции и ошибки.

- 1) оба утверждения верны
- 2) верно только утверждение 2
- 3) верно только утверждение 1
- 4) оба утверждения неверны

## Тема 9. Методы и технологии борьбы с компьютерными вирусами

### 1. Какие существуют методы удаления последствий воздействия вирусов?

- 1) восстановление системы после воздействия известных вирусов
- 2) переустановка операционной системы
- 3) восстановление файлов и загрузочных секторов, зараженных неизвестными вирусами
- 4) способов удаления последствий воздействия вирусов не существует

### 2. Какой из нижеперечисленных вирусов внедряется в операционную систему, и его удаление ведет к ее неработоспособности?

- 1) Kaspersky Security Network
- 2) Adware
- 3) Trojan
- 4) One Half

### 3. Укажите верное утверждение.

1. Аппаратно-программные антивирусные средства обладают рядом достоинств перед программными: работают постоянно; обнаруживают все вирусы, независимо от механизма их действия; блокируют неразрешенные действия, являющиеся результатом работы вируса или неквалифицированного пользователя.

2. Метод вакцинации программ позволяет обнаруживать все вирусы, в том числе и незнакомые.

- 1) оба утверждения верны
- 2) верно только утверждение 2
- 3) верно только утверждение 1
- 4) оба утверждения неверны

### 4. Сопоставьте метод обнаружения вируса с его способом действия.

вакцинация программ (1)	программы определяют и запоминают характеристики всех областей на дисках, в которых обычно размещаются вирусы (6)
применение аппаратно-программных антивирусных средств (2)	создание специального модуля для контроля целостности программы (1)
эвристический анализ (3)	выдает сообщение пользователю о выполнении какой-либо программой подозрительных действий (обращение для записи в загрузочные сектора, помещение в операционных системах резидентных модулей, попытки перехвата прерываний и т.п.) (5)
сканирование (4)	позволяет определять неизвестные вирусы, но не требует предварительного сбора, обработки и хранения информации в файловой системе (3)

использование резидентных сторожей (5)	установление защиты на изменение главной загрузочной записи, загрузочных секторов, файлов конфигурации, исполняемых файлов и др. (2)
обнаружение изменений (6)	программы удаляют обнаруженные вирусы, причем хранят не сигнатуры известных вирусов, а их контрольные суммы (4)

**5. Массовое распространение вирусов вызвало необходимость разработки и использования специальных антивирусных средств для решения следующих задач:**

- 1) блокирование работы программ-вирусов
- 2) составление списка известных вирусов
- 3) устранение последствий воздействия вирусов
- 4) обнаружение всех возможных вирусов

## Тема 10. Криптография

### 1. Для защиты каких данных необходима криптография?

- 1) слухи
- 2) локальная тайна
- 3) государственная тайна
- 4) военная тайна
- 5) врачебная тайна
- 6) коммерческая тайна

### 2. Вставьте пропущенное слово.

Под термином «\_\_\_\_\_» в криптографии понимают сменный элемент шифра, который применяется для шифрования конкретного сообщения.

Ответ: ключ

### 3. Распределите задачи практической криптографии в деловой сфере по направлениям (есть лишние элементы).

Стойкие блочные методы с секретным ключом (1)	для обеспечения секретности и целостности (1)
	для открытого распределения ключей (2)
Нетрадиционные методы сферы защиты информации (2)	для общедоступности данных (лишний элемент)
	для подписи цифрового документа (2)

### 4. Вставьте пропущенное слово.

Идея использовать для целей защиты информации природу объектов микромира, \_\_\_\_\_, поведение которых подчиняется законам физики, стала наиболее актуальной.

Ответ: квантов света.

### 5. Укажите верное утверждение.

1. Основным недостатком симметричного шифрования является то, что секретный ключ должен быть известен отправителю и получателю, что создает новую проблему распространения ключей.

2. В асимметричном шифровании ключи для шифрования и расшифровки разные, хотя и создаются вместе. Один ключ делается известным всем, а другой держится в тайне.

- 1) оба утверждения верны
- 2) верно только утверждение 2
- 3) верно только утверждение 1
- 4) оба утверждения неверны

### 6. Какие методы являются криптографическими средствами защиты?

Ответ: шифрование, кодирование

**7. В квантовой криптографии защита информации, передаваемой по волоконно-оптическим линиям связи (ВОЛС), имеет следующие особенности:**

- 1) обеспечивать передачу фотонов на большие расстояния с минимальными искажениями
- 2) дешевая элементная база
- 3) малая скорость передачи информации
- 4) невозможность подслушать или изменить передаваемую информацию, только путем физического вмешательства в линию передачи

**8. Криптография обеспечивает:**

- 1) конфиденциальность
- 2) доступность
- 3) прозрачность
- 4) актуальность
- 5) подотчетность
- 6) точность



## Тема 11. Биометрия

### 1. Укажите верное утверждение.

1. Уникальная технология 3D-pulse (объемный пульс) дает возможность получать объемные изменения пульсовой волны для расчета физиологических и нервно-психологических характеристик человека с целью контролировать поступки человека.

2. Противники биометрии утверждают, что биометрия – это еще один шаг к обществу тотальной идентификации и контроля каждого гражданина

- а) оба утверждения верны
- б) верно только утверждение 2
- в) верно только утверждение 1
- г) оба утверждения неверны

### 2. Вставьте пропущенное слово.

Биометрические технологии основаны на интеграции исследований в области электроники, информатики, медицины, биометрии. Существует несколько тысяч компьютеризированных мест, хранилищ, исследовательских лабораторий, банков крови, банкоматов, военных сооружений, доступ к которым контролируется устройствами, которые сканируют \_\_\_\_\_ характеристики человека

Ответ: Уникальные

### 3. Надежность работы биометрической системы зависит:

- а) от надежности алгоритма распознавания
- б) от качества ридера
- в) от изменения биометрической характеристики
- г) от размера базы данных
- д) от уникальности и повторяемости характеристик

### 4. Вставьте пропущенное слово.

Вычисление цифрового кода по биометрической характеристике – это процесс \_\_\_\_\_, сам процесс сравнения – это процесс \_\_\_\_\_.

Ответ: оцифровка; распознавания.

### 5. Укажите верное утверждение.

1. Компания «Лазерные системы» разработала BIOCODE-AUTO – противоугонную систему с принципиально новым алгоритмом работы, определяющая не устройство, а человека, владельца автомобиля.

2. Если водителя принуждают завести автомобиль, то у него есть возможность приложить «SOS-палец»: машина заведется, но через некоторое время заглохнет.

- а) оба утверждения верны
- б) верно только утверждение 2
- в) верно только утверждение 1
- г) оба утверждения неверны

**6. Вставьте пропущенное слово.**

Для повышения надежности биометрических систем часто используют не одну, а сразу несколько биометрических характеристик, так называемые \_\_\_\_\_ системы.

Ответ: мультибиометрические

**7. В настоящее время используются следующие биометрические характеристики, кроме:**

- а) радужной оболочки глаза
- б) схемы кровеносных сосудов лица (термограмма лица)
- в) фрагментов генетического кода
- г) папиллярного узора ладони
- д) формы черепа
- е) почерка
- ж) формы кисти руки

**8. Какими функциями обладают биометрические системы, созданные для контроля доступа на секретные объекты?**

- а) учет рабочего времени
- б) контроль рабочего времени
- в) копирование и распространение данных пользователя
- г) идентификации
- д) отслеживание местоположения

**9. Интеллектуальные электронные системы национальной безопасности на основе биометрии установлены для защиты от несанкционированного доступа и нападений:**

- а) в местах скопления народа
- б) на пересечении дорог
- в) в аэропортах
- г) на таможне, пограничных пунктах
- д) на охраняемых объектах
- е) в жилищных комплексах
- ж) на стратегически важных объектах
- з) в институтах и университетах

**10. Принцип действия биометрической системы состоит:**

- а) из опроса пользователя
- б) из алгоритма распознавания
- в) из считывающего устройства (ридера)
- г) из цифрового кода
- д) из биометрической характеристики
- е) из базы данных

## Тема 12. Индивидуальная и государственная защита информации

### 1. Распределите угрозы со стороны интернета по типам.

- а) компульсивное влечение
- б) нарушение прав и законных интересов личности
- в) деформация общественного сознания
- г) построение в интернете пирамидальных мошеннических структур
- д) острая депрессия из-за невозможности вернуться к компьютеру
- е) пропадает чувство времени
- ж) вторжения в потоки конфиденциальной информации юридических лиц и органов власти

- з) синдром вынужденной отмены контактов с компьютером

Информационная (национальная) безопасность государства	Психологическая угроза
а; в; д; е; з	б; г; ж

### 2. Распределите характеристики интернета с точки зрения преимуществ и опасности.

а) позволяет поставщикам программного обеспечения контролировать потоки информации, а также использовать глобальную сеть в интересах стран-лидеров

б) распространение материалы несанкционированного прослушивания юридических и частных лиц

в) является развивающимся информационным средством, стремительно наращивающим свое влияние на людей

г) неподконтролен цензуре, повышает оперативность и свободу

д) дает возможность проведения несанкционированного проникновения в системы управления

е) расширяет возможность государственным и деловым структурам обмениваться информацией с гражданами

ж) позволяет распространять, пропагандировать сектантские идеи

з) делает более доступными учебные материалы, лекции, контакты со специалистами

Преимущества	Опасности
а; г; е; з	б; в; д; ж

### 3. Укажите верное утверждение.

1. Привлечение иностранных инвестиций для опытно-конструкторских работ по созданию отечественных программных и технических средств, обеспечивающих достаточную защищенность баз данных, не несет никаких рисков для России.

2. Для эффективной борьбы с компьютерными преступлениями правоохранительной системе Российской Федерации не требуется сотрудничество с международными организациями.

- а) оба утверждения верны
- б) верно только утверждение 2
- в) верно только утверждение 1
- г) оба утверждения неверны

**4. Какой термин используется для обозначения интернет-зависимости?**

Ответ: Сетемания

**5. Какие из нижеперечисленных защитных мероприятий предлагаются в России для предотвращения угроз в интернете?**

- а) исключительно правоохранительная система Российской Федерации сосредоточена на борьбе с компьютерными преступлениями
- б) повышение общего уровня информационной культуры населения страны
- в) преимущественное использование иностранных технологий и программ, обеспечивающих защиту информации
- г) более четкое определение правового статуса различных информационных объектов, исключаящего бесконтрольное их использование.

## Тема 13. Информационная война

### 1. Выберите верное определение информационной войны:

- а) возможность управления и манипулирования общественным сознанием
- б) нанесение ущерба политической сфере противника и обеспечения собственной безопасности
- в) вид отношений между государствами, при котором для разрешения существующих межгосударственных противоречий используются методы и средства силового воздействия на экономическую сферу этих государств
- г) несогласованная деятельность по использованию информации как оружия для ведения действий в различных сферах: экономической, политической, социальной и на поле боя

### 2. Вставьте пропущенное слово.

\_\_\_\_\_ обращено, прежде всего, к сознанию человека, и уже через него воздействует на убеждения, мотивы и потребности, нравственные установки, отношение к тому, что происходит в обществе.

Ответ: Информационно-психологическое оружие

### 3. Какие разновидности информационных войн выделяются?

- а) оружие массового поражения
- б) экономическое подавление
- в) подавление и уничтожение систем управления
- г) психологическое воздействие на личный состав и население
- д) кибернетическая война
- е) информационное обеспечение боевых действий

### 4. Какими характеристиками обладает информационное оружие?

- а) выбор места и времени применения
- б) не может применяться в мирное время
- в) универсальность, скрытность, широта воздействий
- г) внесение специальных дефектов диверсионного типа (программных закладок)
- д) злонамеренные воздействия на техническую систему
- е) наличие правовых ограничений

### 5. Вставьте пропущенное слово.

\_\_\_\_\_ оружие воздействует на физиологию и психофизиологию человека, минуя сознание.

Ответ: Энергоинформационное

## Тема 14. Информационный терроризм

**1. Террористическое воздействие может осуществляться по одному из трех вариантов. Какой вариант наиболее быстрый?**

- а) на доверенное лицо из внутреннего персонала
- б) с элементами разрушения некоторых компонентов инфраструктуры в среде информационных технологий
- в) по проводной или беспроводной связи (например, радиосвязи).

**2. Надежная система безопасности должна выполнять следующие функции:**

- а) оперативное предотвращение несанкционированного доступа
- б) безопасность данных в аудиторском журнале
- в) контроль работающих приложений
- г) периодическое резервное копирование
- д) фиксация подозрительных событий за время работы системы.

**3. Укажите верное утверждение.**

1. Электромагнитный терроризм использует источники мощных микроволновых излучений, формирующих электромагнитные факторы, достаточные для функционального поражения радиоэлектронных средств (РЭС). Специалистами установлены параметры импульсных потоков радиочастотного электромагнитного излучения микросекундной длительности, наносящих функциональные поражения радиоэлектронной технике, не оказывая при этом соматических биоэффектов в организме человека.

2. Кибертерроризм представляет собой преднамеренную политически мотивированную атаку на информацию, вычислительные системы, компьютерные программы или данные. Системы спутниковой связи и глобальные сети (в первую очередь интернет) не способствуют развитию этого вида терроризма.

- а) оба утверждения верны
- б) оба утверждения неверны
- в) верно только утверждение 2
- г) верно только утверждение 1

**4. Сопоставьте период и используемый в то время термин для определения безопасности в информационных системах.**

*Соедините элементы попарно:*

- 1. 1970-е гг. а) «защита информации»
- 2. до 1960-х гг. б) «безопасность данных»
- 3. начало XXI в. в) «компьютерная безопасность»
- 4. 1960-е гг. г) «информационная безопасность»

1	2	3	4
б	а	в	г

**5. Вставьте пропущенное слово.**

В XXI веке может появиться новый вид терроризма – программирование требуемого поведения и деятельности целых групп населения, например, \_\_\_\_\_ на основе виртуальной реальности.

Ответ: видеоигры

## Тема 15. «Особенности управления информации в городах»

### 1. Укажите верное утверждение.

1. ЕДДС города не несет ответственности за своевременность принятия необходимых экстренных мер по защите и спасению людей, материальных и культурных ценностей.

2. ЕДДС города должна включать в себя дежурно-диспетчерский персонал, пункт управления, технические средства автоматизации управления, связи и оповещения.

- а) оба утверждения верны
- б) верно только утверждение 1
- в) верно только утверждение 2
- г) оба утверждения неверны.

### 2. Вставьте пропущенное слово.

Каждую единую объединенную диспетчерскую систему (например, «911» в США и «112» в Европе) можно разделить на \_\_\_\_\_ часть, под которой подразумевается координация действий и интеграция всех служб оперативного реагирования, и на \_\_\_\_\_ часть, в которую входит сам центр управления, средства связи, включая телефонную, оперативную радиосвязь, сотовую и спутниковую связь, средства определения местоположения подвижных объектов, системы передачи цифровой информации.

Ответ: организационную; техническую

### 3. Что входит в основные задачи ЕДДС (единые дежурно-диспетчерские системы)?

**Оценка и контроль обстановки, подготовка вариантов управленческих решений по ликвидации чрезвычайной ситуации, принятие необходимых решений (в пределах установленных вышестоящими органами полномочий)?**

а) утаивание информации об угрозе или возникновении чрезвычайной ситуации, о сложившейся обстановке

б) анализ и оценка достоверности поступившей информации, доведение ее до ДДС, в компетенцию которых входит реагирование на принятое сообщение

в) сбор от дежурно-диспетчерских служб, служб контроля и наблюдения (систем мониторинга) за окружающей средой и распространение между ДДС города информации об угрозе или факте возникновения чрезвычайной ситуации

г) факт возникновения чрезвычайных ситуаций различного характера

### 4. Вставьте пропущенное слово.

ЕДДС и дежурно-диспетчерские службы, входящие в ОСОДУ города, функционируют в трех режимах: \_\_\_\_\_ деятельности, повышенной готовности и чрезвычайной ситуации.

Ответ: повседневной



**5. Для решения внезапной ситуации существуют службы оказания помощи населению в чрезвычайных ситуациях (спасательная служба, скорая медицинская помощь, противопожарная служба, полиция и др.). Для работы этих служб важны следующие общие моменты:**

- а) скорость реагирования системы
- б) предотвращение ситуации
- в) единственное ответственное лицо
- г) комплексный характер требуемой помощи
- д) зависимость от времени поступления, объема и достоверности

## **Тема 16. Особенности обеспечения информационной безопасности Российской Федерации в различных сферах общественной жизни**

**1. Информационная безопасность Российской Федерации оказывает влияние на защищенность национальных интересов в сфере экономики. Воздействию угроз в сфере экономики наиболее подвержены:**

- a) электронная книга доходов и расходов семьи
- b) системы сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации и информации о внешне-экономической деятельности государства
- c) система государственной статистики
- d) системы бухгалтерского учета предприятий, учреждений и организаций независимо от формы собственности
- e) кредитно-финансовая система
- f) фондовый рынок

### **2. Выберите один правильный ответ**

Информационно-пропагандистская деятельность политических сил, общественных объединений, СМИ и отдельных лиц, искажающая стратегию и тактику РФ, и нарушение установленного порядка сбора, обработки, хранения и передачи информации в федеральных органах исполнительной власти РФ относятся к А) \_\_\_\_\_ угрозам информационной безопасности в сфере Б) \_\_\_\_\_ РФ.

Под буквой А:

- a) Внешним
- b) Внутренним
- c) Информационным
- d) Политическим

Под буквой Б:

- a) Экономики
- b) Внешней политики
- c) Внутренней политики
- d) Науки и техники

**3. Укажите, при каких условиях возможны угрозы несанкционированного доступа в информационной безопасности РФ:**

- a) при сохранении информации, содержащей коммерческую тайну
- b) при бесконтрольной деятельности новых коммерческих структур по созданию и защите систем сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации
- c) при ответственности хозяйствующих субъектов за недостоверность сведений об их коммерческой деятельности
- d) при критическом состоянии предприятий, разрабатывающих и производящих средства информатизации, телекоммуникации, связи и защиты процессов переработки информации

е) при компьютерных преступлениях, связанных с проникновением криминальных элементов в компьютерные системы и сети банков и иных кредитных организаций

**4. Укажите верное утверждение.**

1. Реальный путь противодействия угрозам информационной безопасности РФ в области науки и техники – это совершенствование законодательства Российской Федерации, регулирующего отношения в данной области, и механизмов его реализации.

2. Наибольшую опасность в сфере духовной жизни представляет деформация системы массового информирования как за счет монополизации средств массовой информации, так и за счет неконтролируемого расширения сектора зарубежных средств массовой информации в отечественном информационном пространстве.

- а) Выберите один правильный ответ
- б) оба утверждения верны
- в) верно только утверждение 1
- г) оба утверждения неверны
- д) верно только утверждение 2

**5. Что из нижеперечисленного не относится к основным направлениям обеспечения информационной безопасности РФ в общегосударственных информационных и телекоммуникационных системах?**

а) исключение несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации

б) предотвращение перехвата информации из помещений и с объектов, а также информации, передаваемой по каналам связи с помощью технических средств

в) неприкосновенность информации, передаваемой по каналам связи с помощью технических средств

г) предотвращение утечки информации по техническим каналам, возникающей при эксплуатации технических средств ее обработки, хранения и передачи

## Тема 17. Информационная экономика

### 1. В чем выгода использования intranet?

- 1) мгновенная публикация данных на ресурсах intranet
- 2) постоянно меняющийся код доступа
- 3) легкий доступ персонала к данным
- 4) высокая производительность при совместной работе над общими проектами
- 5) ограниченное время пользования

### 2. Какие утверждения из нижеперечисленных относятся к основным принципам политики информационной безопасности?

- 1) компьютер никогда не остается без присмотра включенным
- 2) использование нелицензионного программного обеспечения
- 3) любой пользователь может использовать компьютер любого сотрудника
- 4) никто не может увидеть ни одного файла с компьютера сотрудника по сети

### 3. Что из нижеперечисленного *не относится* к недостаткам intranet-сети?

- 1) распространение нелегитимных и оскорбительных материалов
- 2) введение общей корпоративной культуры
- 3) значительные накладные расходы на разработку и администрирование сети intranet
- 4) утечка к конкурентам корпоративных данных через недобросовестного работника

### 4. Как называется внутренняя частная сеть организации или крупного государственного ведомства?

Ответ: ИнтАрнет

## Тема 18. Глобальная информатизация общества

### 1. Вставьте пропущенное слово.

Объективные предпосылки глобализации информационного общества связаны \_\_\_\_\_ достижениями революции, а затем – революции в информационной и \_\_\_\_\_ сфере.

- а) Научно-технической
- б) информационной

### 2. Выберите один или несколько правильных ответов

Унификация человека как глобальная угроза безопасности содержит следующие тезисы:

- а) ожидание готовых решений – желательно простых, четких, как воинские команды
- б) создание «человека-зомби», управляемого через средства коммуникации
- в) попадание под влияние магической власти призывов «ради общего дела»
- г) понимание информации и развитие критического мышления
- д) принятие субъектом ответственности за происходящее

### 3. Какое социальное деление сформировалось в структуре нового общества к концу XX века? Сопоставьте классы с характеристикой.

Соедините элементы попарно:

- 1) привилегированный класс
- 2) бедный класс
- 3) «средний класс»

а) люди, заработок которых позволяет обеспечить семью, но для этого им приходится трудиться в нескольких местах, не имея времени ни на что иное, кроме работы

б) представители владеют основными общественными богатствами, имеют более высокий интеллектуальный потенциал

в) исполнители наиболее непривлекательных видов труда при условии, если у них есть работа

Ответ

- 1) б
- 2) в
- 3) а
- 4) 5.

### 4. Вставьте пропущенное слово.

Главная угроза социальной безопасности на фоне глобализации – быстро оформляющееся социальное \_\_\_\_\_ населения.

Ответ: Расслоение

### **5. Укажите верное утверждение.**

1. Качественная дифференциация уже происходит между людьми (внутри населения отдельных стран) и между странами. Главной целью такого порядка является осуществление контроля над людьми и лучшей управляемости людьми.

2. «Глобальное общество» формирует единое мышление, оно всегда сориентировано на упрощенную интерпретацию происходящего. При таком развитии людям становится свойственно критическое мышление и анализ получаемой информации.

- а) оба утверждения верны
- б) верно только утверждение 2
- в) верно только утверждение 1
- г) оба утверждения неверны

## Тема 19. Воздействие средств массовой информации

### 1. Вставьте пропущенное слово.

Метод воспитания «\_\_\_\_\_ мышления» способствуют развитию у детей навыка критического мышления, учит их находить ответы с помощью логично выстраиваемых учителем вопросов.

Ответ: критического

### 2. Кто автор утверждения, что «воздействие СМИ на психику человека по силе равно взрыву атомной бомбы»?

- a) Ги Дебор
- b) Э. Бароло
- c) Б.Е. Гершунский
- d) А.М. Новиков

### 3. Что Т.Е. Кабаченко рассматривает как источник нарушения информационно-психологической безопасности личности и общества?

- a) ровесники
- b) выступления артистов
- c) профессиональные СМИ
- d) аппарат управления страны

### 4. Метод аналитического подхода к СМИ опирается на серию логично выстраиваемых вопросов. Распределите вопросы в правильном порядке.

*Расставьте в правильном порядке*

- a) кто сообщает? (анализ управления)
- b) кому сообщает? (анализ аудитории)
- c) что сообщает? (анализ содержания)
- d) с каким успехом сообщает? (анализ результата)
- e) с какой целью сообщает? (анализ цели)
- f) по какому каналу сообщает? (анализ средства)

Ответ: a, c, f, b, e, d

## Тема 20. Реклама как источник информационной опасности

**1. Какие плюсы можно выделить у потока рекламы? Выберите один или несколько правильных ответов**

- 1) реализация небольших, но полезных социальных проектов
- 2) поднятие настроения себе и окружающим
- 3) длинный перерыв на личные дела
- 4) пропаганда здорового образа жизни, нравственных ценностей
- 5) дезинформация об условиях предоставления услуги

**2. Укажите верное утверждение.**

1) Рекламные картинки «красивой жизни» формируют определенную структуру ценностей, в которой уделяется значительное место духовности, высоким нравственным целям, таким качествам, как доброта, справедливость, человечность, альтруизм.

2) Реклама – спаситель. Она поможет найти нечто важное и нужное для жизни, приведет к счастью.

- 1) оба утверждения верны
- 2) верно только утверждение 2
- 3) верно только утверждение 1
- 4) оба утверждения неверны

**3. Что такое реклама?**

- 1) форма развлекательного контента
- 2) психологическое программирование людей на приобретение товара и услуг
- 3) справочное пособие для потребителя
- 4) сравнительная характеристика товаров и услуг

**4. Укажите приемы рекламного воздействия на сознание среди нижеперечисленного:**

- 1) придание наукообразного вида с помощью графиков, таблиц
- 2) инструмент систематического и изоциренного психологического насилия
- 3) эксплуатация желания людей «быть уникальным»
- 4) внушение мифа о рекламе как двигателе прогресса
- 5) сказанное один раз воспринимается как истина
- 6) исполнение ролей героев рекламных роликов артистами, политиками

**5. Как называется реклама, в которой используется прием «25-го кадра»?**

Ответ: Подпороговая реклама



## Тема 21. Ложь как источник информационной опасности

### 1. Выделите признаки ложного высказывания по В.В. Зеньковскому:

- а) автор высказывания осознанно стремится ввести кого-либо в заблуждение
- б) ложное высказывание содержит некоторую долю истины
- в) автор высказывания не желает придать ложной мысли вид истины
- г) ложное высказывание искажает объективное представление о действительности
- д) автор высказывания заведомо знает, что данное высказывание ложно

### 2. Вставьте пропущенное слово.

Ложь – значимый скрытый элемент больших и малых \_\_\_\_\_ войн.

- а) Информационных

### 3. Какой из подходов ко лжи недопустим?

- а) Философ В.С. Соловьев считал возможным нравственную ложь во спасение.
- б) Платон, Г. Гегель, Н. Макиавелли считали, что ложь возможна «во благо общества».
- в) А. Шопенгауэр называл отрицание необходимой лжи «жалкой заплатой на одежде убогой морали».
- г) Вольтер считал, что ложь – высшая добродетель, причем нужно лгать не робко, не время от времени, а смело и всегда.
- д) Ф. Ницше говорил, что «обман имеет целью спасти нас от самих себя».

### 4. Какие термины используются для описания методов, основанных на лжи и используемых в экстремальных условиях войн, в боевой обстановке?

- а) ложные позиции
- б) ложные высказывания
- в) донос
- г) ложные сообщения
- д) белая ложь

### 5. Укажите верное утверждение.

- 1. В современных информационных войнах ложь теряет свое значение.
  - 2. Стратегически ложь всегда, в любых ситуациях сильнее правды.
- а) оба утверждения верны
  - б) верно только утверждение 2
  - в) верно только утверждение 1
  - г) оба утверждения неверны

## Тема 22. Информационные образовательные технологии XXI века

### 1. В век дистанционного обучения требуется:

- a) высокий культурный уровень
- b) информационная подготовка
- c) технологическая грамотность
- d) профессиональная подготовка
- e) высокий уровень эмоционального интеллекта

### 2. Дистанционная форма обучения сегодня дает возможность создания:

- a) всеобщего обмена информацией
- b) систем массового непрерывного самообучения
- c) зависимости от временных поясов
- d) независимости от пространственных поясов

### 3. Что из нижеперечисленного не относится к дидактическим принципам организации дистанционного обучения?

- a) индивидуализация обучения
- b) наглядность
- c) системность и систематичность
- d) развитие личности

### 4. Что из нижеперечисленного относится к задачам дистанционного обучения?

- a) обратная связь между обучаемым и учебным материалом
- b) развитие эмоционального интеллекта
- c) возможность обучения в группе
- d) доставка необходимых учебных материалов
- e) самостоятельная ориентировка в информации

### 5. Что из нижеперечисленного относится к числу проблем организации дистанционного обучения?

- a) создание нормативно-правовой базы оценки знаний учащихся
- b) технологические проблемы со стороны учащихся
- c) информационное перенасыщение человека (проблема экологически чистой информационной среды)
- d) географическое расположение учащихся
- e) подготовка специалистов и преподавателей, владеющих современными педагогическими и информационными технологиями

### 6. Вставьте пропущенное слово.

Дистанционное обучение на основе \_\_\_\_\_ программ ориентировано на обучение взрослой аудитории, тех людей, которые по каким-то причинам не смогли закончить школьное образование.

Ответ: мультимедийных

## Тема 23. Информационная экология

**1. Представление об устойчивом развитии общества в России чаще всего принимают в соответствии с определением комиссии «Наше общее наследие». Оно подчеркивает следующие важнейшие факты:**

- 1) необеспеченность потребностей человечества в настоящем времени, так как четверть населения мира жила и живет за чертой бедности
- 2) продолжающееся разрушение окружающей среды, в первую очередь естественных экосистем, и направленные изменения концентрации биогенов и других веществ во всех средах
- 3) развитие общества порождает дискуссию, может ли развитие быть устойчивым
- 4) слабое обеспечение информационной безопасности
- 5) последовательное истощение ресурсов и исчезновение, например, возобновляемых ресурсов

### **2. Укажите верное утверждение.**

1. В России давно обсуждается проблема ноосферного пути развития, восходящая к трудам В.И. Вернадского. Сейчас делаются попытки увязки ноосферного пути развития, поэтому в определенной степени с термином «устойчивое развитие» в России конкурирует понятие «ноосфера».

2. Устойчивое развитие, согласно теории биотической регуляции окружающей среды, означает «улучшение качества жизни людей, живущих в пределах несущей емкости поддерживающих экосистем».

- а) оба утверждения верны
- б) верно только утверждение 2
- в) верно только утверждение 1
- г) оба утверждения неверны

**3. Экологическая информация означает сведения в письменной, аудиовизуальной, электронной или любой иной материальной форме:**

- а) об информационных технологиях
- б) о факторах, таких как вещества, энергия, шум и излучение
- в) о состоянии элементов окружающей среды, таких как воздух и атмосфера, вода, почва, земля, ландшафт и природные объекты, биологическое разнообразие и его компоненты, включая генетически измененные организмы, и взаимодействия между этими элементами
- г) о государственных и коммерческих тайнах
- д) о состоянии здоровья и безопасности людей, условиях их жизни, состоянии объектов культуры, зданий и сооружений

**4. Выберите определение понятия «устойчивое развитие», используемое в законодательстве РФ:**

а) развитие общества, которое позволяет удовлетворять потребности нынешних поколений, не нанося при этом ущерба возможностям, оставляемым в наследство будущим поколениям для удовлетворения их собственных потребностей

б) гармоничное развитие производства, социальной сферы, населения и окружающей природной среды

в) управление совокупным капиталом общества в интересах сохранения и приумножения человеческих возможностей

г) модель поступательного развития общества, при которой достигается удовлетворение жизненных потребностей нынешнего поколения без лишения такой возможности, будущих поколений людей

**5. Управление информацией в городской среде, в отличие от природных комплексов, предполагает принятие управляющих решений в течение А)\_\_\_\_\_, а осуществление управляющих воздействий – в течение Б)\_\_\_\_\_.**

Ответы:

А) 1. пары часов

2. Нескольких дней

3. месяца

4. Трех лет

Б) 1. Пары часов

2. Нескольких дней

3. месяца

4. Трех лет

## Тема 24. Географические информационные системы

### 1. Укажите верное утверждение:

1. Дистанционные методы изучения окружающей среды (ДЗЗ) – это специфический метод дистанционного зондирования с помощью аэрофотосъемки.

2. ГИС обеспечивают уникальные возможности для ее применения в широком спектре задач, связанных с анализом и прогнозом явлений и событий окружающего мира.

- a) оба утверждения верны
- b) верно только утверждение 2
- c) верно только утверждение 1
- d) оба утверждения неверны

### 2. Вставьте пропущенное слово.

Для автоматического определения местоположений объектов применяется процедура под названием «\_\_\_\_\_», чтобы определить и посмотреть на карте, где находится интересующий объект или явление.

Ответ: геокодирование

### 3. Задача, которая не решается с помощью ГИС:

- a) поиск и рациональное использование природных ресурсов
- b) обыкновенный анализ
- c) мониторинг экологических ситуаций
- d) ведение комплексного и отраслевого кадастра
- e) картографирование
- f) контроль условий жизни населения

### 4. Укажите, что является основными достоинствами дистанционного мониторинга:

a) невозможность проследить глобальные и крупные региональные особенности природы Земли

b) космические снимки дают однотипную информацию о трудно-доступных районах

c) системный характер информации

d) мгновенность изображения обширных площадей сводит к минимуму влияние переменных факторов

e) регистрируются сведения об обширных пространствах вплоть до всей видимой в момент съемки части Земного шара

f) по материалам повторных съемок изучается динамика природных процессов

**5. Научным обоснованием, проектированием, созданием, эксплуатацией и использованием ГИС, разработкой геоинформационных технологий и прикладными аспектами или приложениями ГИС для практических или научных целей занимается:**

- a) геоинженерия
- b) геоинформатика
- c) география

**6. Геоинформационная система (ГИС) - это:**

- a) изучение с помощью новых технологий объектов реального мира
- b) анализ событий Земли
- c) прогноз явлений окружающего мира
- d) управление окружающей средой и обществом
- e) картографический банк данных
- f) пространственный анализ карты

**7. Укажите функциональные возможности ГИС:**

- a) картометрические операции
- b) ввод данных без оцифровки источников данных
- c) ввод данных в машинную среду путем импорта из существующих наборов цифровых данных
- d) трансформацию картографических проекций, изменение систем координат
- e) работа с данными без преобразования и конвертации
- f) хранение, манипулирование и управление данными в базах

**8. ГИС-технология не объединяет традиционные операции работы:**

- a) со статистическим анализом
- b) с базами данных
- c) с географическим (пространственным) анализом
- d) с традиционной визуализацией

**9. Вставьте пропущенное слово.**

ГИС развивались на базе информационно-поисковых систем и позднее на основе \_\_\_\_\_ банков данных.

Ответ: картографических

## **Тема 25. Актуальные вопросы обеспечения безопасности и развития детей в информационном пространстве**

### **1. Какой термин используется для описания кражи личных данных**

Ответ: фишинг

### **2. Какая информация не причиняет вред здоровью и развитию детей?**

- 1) оправдывающая противоправное поведение
- 2) побуждающая детей принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством
- 3) побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству
- 4) побуждающая осуществлять насильственные действия по отношению к людям или животным
- 5) формирующая семейные ценности и уважение к родителям

### **3. Какой пароль лучше всего подойдет для аккаунта в сети?**

- 1) 39Mrd91V\$
- 2) 1q2w3e4r
- 3) il0vemym0m
- 4) dimapetrov

### **4. Выберите способы контроля деятельности ребенка в интернете с помощью специального программного обеспечения:**

- 1) чистка журнала просмотренных веб-страниц.
- 2) настройки безопасного поиска (установка запрета на открывание сайтов определенной тематики) и защита их паролем
- 3) программы фильтрации
- 4) родительский контроль
- 5) контентные фильтры (установка запрета на определенное содержание)
- 6) ситуационные задачи

### **5. В чем выражается кибербуллинг?**

- 1) преследование сообщениями
- 2) агрессия
- 3) игнорирование негатива
- 4) оскорбление пользователей сети
- 5) подпись в конце электронного письма

### **6. В чем заключается информационная безопасность ребенка?**

- 1) общественное давление
- 2) риск нарушения физического и психического здоровья, духовного и нравственного развития
- 3) присутствует риск причинить вред ребенку информацией
- 4) состояние защищенности детей

*Учебное издание*

Мухин Алексей Арьевич

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

Сборник контрольных заданий (тестов)

Авторская редакция

Компьютерная верстка: В.В. Данилова

Издательский центр «Удмуртский университет»  
426034, г. Ижевск, ул. Ломоносова, 4Б, каб. 021  
Тел. : + 7 (3412) 916-364, E-mail: [editorial@udsu.ru](mailto:editorial@udsu.ru)