ПРОФИЛЬ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

8-9 класс

Тестовые задания

I. Общая часть

1. Назовите метод перестановки компонентов проектирования объекта, который позволяет найти новое в проектировании за счёт изменения взгляда на объект творчества.

1) декомпозиция
2) фрагментация
3) инверсия
4) дифференциация

2. Укажите технологии создания объектов, деталей или вещей путем добавления материала:

1) аддитивные
2) наукоемкие
3) субтрактивные
4) промышленные

3. К какому виду классификации информационных технологий относятся следующие способы обработки информации: сканирование, распознавание, трансформирование информации.

1) по форме представления информации
2) по методам обработки информации
3) по средствам осуществления коммуникации
4) по способу передачи информации

4. Назовите определение поступательного, взаимообусловленного развития науки и техники на протяжении истории.

1) научно-технический регресс
2) научно-технический прогресс
3) научно-технический процесс
4) научно-техническая революция

5. Выполнение проекта начинается с

1) выбора оптимальной идеи реализации проекта
2) разработки конструкции изделия
3) разработки технологии изготовления изделия
4) определения проблемы и темы проекта

II. Специальная часть
профиль «Информационная безопасность»

6. Под «информационной безопасностью» понимают:

1) защиту от несанкционированного доступа

2) защиту информации от случайных и преднамеренных воздействий естественного и искусственного характера

3) защиту информации от компьютерных вирусов

4) предотвращение санкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации.

7. Что понимается под «фишинговой атакой»?

1) подбор пароля

2) кража учетных данных с помощью фальшивых сайтов, маскирующихся под настоящие

3) взлом аккаунта с помощью ответа на контрольный вопрос

8. Какие программы называются эксплойтами?

1) вредоносные программы, которые маскируются под полезные

2) программы, которые используют уязвимости в программном обеспечении с целью навредить компьютеру

3) программы, которые срабатывают только в определенное время, и, незаметно для пользователя, вредят другим пользователям сети.

9. Укажите какие свойства информации должна обеспечивать информационная безопасность?

1) конфиденциальность

2) точность

3) зашифрованность

4) полноту

5) доступность

6) блокированность

10. Выберите наиболее эффективное средство для защиты от сетевых атак.

1) использование сетевых экранов или «firewall»

2) использование антивирусных программ

3) посещение только «надёжных» Интернет-узлов

4) использование только сертифицированных программ-броузеров при доступе к сети Интернет

11. Что такое брутфорс?

1) подбор пароля

2) кража учетных данных с помощью фальшивых сайтов, маскирующихся под настоящие

3) взлом аккаунта с помощью ответа на контрольный вопрос

12. Укажите методы повышения достоверности входных данных.

1) замена процесса ввода значения процессом выбора значения из предлагаемого множества
2) отказ от использования данных
3) проведение комплекса регламентных работ
4) использование вместо ввода значения его считывание с машиночитаемого носителя
5) введение избыточности в документ первоисточник
6) многократный ввод данных и сличение введенных значений

13. Основные угрозы доступности информации:

1) непреднамеренные ошибки пользователей
2) злонамеренное изменение данных
3) хакерская атака
4) отказ программного и аппаратного обеспечения
5) разрушение или повреждение помещений
6) перехват данных

14. Укажите разделы современной криптографии.

1) симметричные криптосистемы
2) криптосистемы с открытым ключом
3) криптосистемы с дублированием защиты
4) системы электронной подписи
5) управление паролями
6) управление передачей данных
7) управление ключами

15. Укажите основные угрозы конфиденциальности информации.

1) маскарад
2) карнавал
3) переадресовка
4) перехват данных
5) блокирование
6) злоупотребления полномочиями

16. Выделите сервисы безопасности.

1) идентификация и аутентификация
2) шифрование
3) инверсия паролей
4) контроль целостности
5) регулирование конфликтов
6) экранирование
7) обеспечение безопасного восстановления
8) кэширование записей

17. Под угрозой удаленного администрирования в компьютерной сети понимается угроза

1) несанкционированного управления удаленным компьютером

2) внедрения агрессивного программного кода в рамках активных объектов Web-страниц

3) перехвата или подмены данных на путях транспортировки

4) вмешательства в личную жизнь

5) поставки неприемлемого содержания

18. Выберите все понятия, являющиеся видами кибератак.

1) DDOS-атака

2) Спуфинг

3) Вандализм

4) Социальная инженерия

5) Кибервойны

6) Кража личности

19. Дима записал IP-адрес школьного сервера на листке бумаги и положил его в карман куртки. Димина мама случайно постирала куртку вместе с запиской. После стирки Дима обнаружил в кармане четыре обрывка с фрагментами IP-адреса. Эти фрагменты обозначены буквами А, Б, В и Г. Восстановите IP-адрес. В ответе укажите последовательность букв, обозначающих фрагменты, в порядке, соответствующем IP-адресу.

5.211	11	3.12	.47
А	Б	В	Г

***Ответ*: _____.**

20. Вирусный аналитик столкнулся с файлом, зашифрованным вирусом-шифровальщиком. Одна из строк файла выглядела следующим образом:

ЛРЧСУПГЩЛСРРГВ ДЗКСТГФРСФХЯ

Определите использованный вирусом шифр и восстановите первоначальный текст в данной строке.

***Ответ*:** шифр _____.
Восстановленный текст – _____.

А	Б	В	Г	Д	Е
Ё	Ж	З	И	Й	К
Л	М	Н	О	П	Р
С	Т	У	Ф	Х	Ц
Ч	Ш	Щ	Ъ	Ы	Ь
Э	Ю	Я			

III. Кейс-задание

21. Творческое задание.

Инструкция. Прочитайте описание ситуации и ответьте на вопросы.

Ситуация. Иванов и Петров, используя вредоносную программу, позволяющую удаленно управлять компьютером, который был заражен терминал одного из банков, перевели денежные средства на сумму свыше 10 млн. рублей на счет своей банковской карты.

Вопросы.

1. Являются ли описанные в задачах действия правонарушениями?
2. Если да, то квалифицируйте их.