ПРОФИЛЬ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

10-11 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. Укажите, в чем заключается принципиальное отличие межсетевых экранов (МЭ) от систем обнаружения атак (СОВ).

1) МЭ были разработаны для активного или пассивного обнаружения, а СОВ – для активной или пассивной защиты

2) МЭ были разработаны для активной или пассивной защиты, а СОВ – для активного или пассивного обнаружения

3) МЭ работают только на сетевом уровне, а СОВ – еще и на физическом

11. Соотнесите основные понятия в области информационной безопасности:

1. Атака	А. Некоторое неудачное свойство системы, которое делает возможным возникновение и реализацию угрозы.
2. Уязвимость автоматизированной системы (АС)	Б. Система со средствами защиты, которые успешно и эффективно противостоят угрозам безопасности.
3.Угроза безопасности АС	В. Возможные воздействия на АС, которые прямо или косвенно могут нанести ущерб ее безопасности.
4. Защищенная система	Г. Действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы

Ответ: 1-___; 2-___; 3-____; 4-____.

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. Укажите 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. Выделите 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. Продолжите фразу: «Последовательность символов, недоступная для посторонних, предназначенная для идентификации и аутентификации субъектов и объектов между собой – это …».

Ответ: _____.

19. Для некоторой подсети используется маска 255.255.224.0. Как известно на практике два из возможных адресов не используются для адресации узлов сети: адрес сети, в котором все биты, отсекаемые маской, равны 0, и широковещательный адрес, в котором все эти биты равны 1. Сколько различных адресов компьютеров допускает эта маска?

Ответ: _____.

20. Вирусный аналитик столкнулся с файлом, зашифрованным вирусом-шифровальщиком. Аналитику удалось определить ключевое слово: «*ВИРУС*». Одна из зашифрованных строк файла выглядела следующим образом:

УНГШУВЗ СШЩРШРЕЯРЪГП

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 выполните задание.

Ситуация. Вас пригласили в качестве консультанта по безопасности в офис компании ООО “КИБЕРНЕТИКА”. В компании недавно произошла утечка базы данных клиентов, и директор фирмы всерьез задумался о безопасности коммерческих данных. Системный администратор организации сообщил следующее:

Организация имеет один центральный офис и удаленный филиал. В центральном офисе находятся кабинет директора, кабинеты отдела продаж и бухгалтерии. Филиал находится в другом городе и подключается к программе «1С», установленной на сервере через службу терминалов по протоколу RDP. На сервере установлен контроллер домена. Из соображений безопасности пользователи работают в доменных учетных записях. В кабинете директора установлен Wi-Fi-роутер, играющий роль шлюза всей офисной сети. Директор подключается к нему через Wi-Fi с личного ноутбука. Так же для выхода в Интернет данной Wi-Fi сетью пользуются клиенты организации.

Wi-Fi роутер

WAN Провайдер, DHCP client, включен NAT(PAT), firewall, проброшен порт RDP 3389 на сервер 192.168.0.2

LAN 192.168.0.1

DHCP-Server Отключен

Wireless SSID: MegaOffice

Security: WPA Personal/TKIP

Password: 13467925

В отделе продаж установлено два компьютера, в бухгалтерии два компьютера и сервер. Все эти устройства подключены к коммутатору, установленному на этаже. На сервере установлена Windows Server 2008R2 и серверная часть «1С: Предприятие 8.2». С «1С» работают сотрудники отдела продаж, бухгалтерии, а также иногда подключается директор предприятия. К «1С» подключение осуществляется через тонкий клиент 1С.

Server AD+1C
IP-адрес 192.168.0.2
Роль DHCP сервер Область 192.168.0.100-254
Шлюз 192.168.0.1 DNS 192.168.0.2 8.8.8.8
Lease time 5d
Роль DNS сервер Зона "domain.local"
Роль контроллер AD Домен "domain.local"
Роль сервер терминалов

Существует также удаленный офис, находящийся в другом городе. Сеть его состоит из одного концентратора, маршрутизатора (подключенного к сети провайдера) и двух компьютеров менеджеров, работающих с «1С» установленной на сервере в бухгалтерии. Компьютеры не находятся в корпоративном домене.

Задание. Проанализируйте существующую сеть предприятия и укажите возможные проблемы в безопасности.