**ЗАДАНИЕ 1**

1 – А

2 – Г

3 – А

4 – А

5 – Б

6 – Г

7 – Д

8 – Е

9 – А

10 – А

11 – А  
12 – А

13 – В

14 – Г

15 – А

16 – Б

17 – А

18 – Б

19 – Б

20 – А

21 – Б

22 – В

23 – Б

24 – А

25 – А

26 – Г

27 – Д

28 – Е

29 – Г

30 – А

31 – Б

32 – Е

33 – А

34 – Г

35 – Г

**ВОПРОС 1.**

«Под информационной безопасностью будем понимать защищенность информации и …………….. от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры»

а) поддерживающей инфраструктуры

б) человека

в) конфиденциальных данных

**ВОПРОС 2.** Защита информации – это …

а) комплекс мероприятий, направленных на обеспечение информационной безопасности

б) совокупность методов, средств и мер, направленных на обеспечение информационной безопасности общества, государства и личности во всех областях их жизненно важных интересов

в) комплекс мероприятий, проводимых собственником информации, по ограждению своих прав на владение и распоряжение информацией, созданию условий, ограничивающих ее распространение и исключающих или существенно затрудняющих несанкционированный, незаконный доступ к засекреченной информации и ее носителям

г) все определения корректны

**ВОПРОС 3.** Действия по определению конкретных угроз и их источников, приносящих тот или иной вид ущерба называются:

а) обнаружение угроз

б) пресечения и локализация угроз

в) ликвидация угроз

**ВОПРОС 4**. Возможность за приемлемое время получить требуемую информационную услугу называется:

а) доступностью информации

б) целостностью информации

в) предоставлением информации

**ВОПРОС 5.** Актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения называется:

а) доступностью информации

б) целостностью информации

в) предоставлением информации

г) конфиденциальностью информации

**ВОПРОС 6.** Нарушение какого из аспектов информационной безопасности влечет за собой искажение официальной информации, например, текста закона, выложенного на странице Web-сервера какой-либо правительственной организации

а) доступность информации

б) целостность информации

в) предоставление информации

г) конфиденциальность информации

**ВОПРОС 7.** Меры каких уровней НЕ входят в организацию системы обеспечения информационной безопасности:

а) законодательного уровня

б) административного уровня

в) процедурного уровня

г) программно-технического уровня

д) программно-аппаратного уровня

**ВОПРОС 8.** Многообразие нормативных документов представлено международными, национальными, отраслевыми нормативными документами. Какая организация НЕ занимается вопросами формирования законодательства в сфере информационных ресурсов?

а) ISO

б) ITU

в) АNSI

г) NIST

д) NASA

е) SWIFT

ж) GISA

**ВОПРОС 9.** Вопросы сертификации и лицензирования средств обеспечения информационной безопасности в России рассматривает:

а) Федеральная служба по техническому и экспортному контролю при Президенте РФ

б) Федеральная служба безопасности Российской Федерации

в) Служба внешней разведки Российской Федерации

**ВОПРОС 10.** Совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов принято считать:

а) политикой безопасности

б) методами защиты информации

в) ограничением доступа к информации

учетными записями пользователей

**ВОПРОС 11.** Потенциальная возможность определенным образом нарушить информационную безопасность – это ….

а) угроза

б) атака

в) взлом

**ВОПРОС 12.** Источниками угрозы называют …

а) потенциальных злоумышленников

б) компьютерные вирусы

в) глобальную сеть Интернет

**ВОПРОС 13.** Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется …

а) окном безопасности

б) окном опасности

в) скользящим окном

г) окном угрозы

**ВОПРОС 14.** Ошибки программного обеспечения с точки зрения информационной безопасности являются:

а) уязвимым местом

б) окном опасности

в) окном безопасности

г) источником угрозы

**ВОПРОС** **15.** Ошибки администрирования системы с точки зрения информационной безопасности являются:

а) уязвимым местом

б) окном опасности

в) окном безопасности

г) источником угрозы

**ВОПРОС** **16.** Ошибка в программе, вызвавшая крах системы с точки зрения информационной безопасности являются:

а) уязвимым местом

б) окном опасности

в) окном безопасности

г) источником угрозы

**ВОПРОС** **17.** Некоторая уникальная информация, позволяющая различать пользователей называется:

а) идентификатор (логин)

б) пароль

в) учетная запись

г) ключ

**ВОПРОС** **18.** Некоторая секретная информация, известная только пользователю и парольной системе, которая может быть запомнена пользователем и предъявлена парольной системе называется:

а) идентификатор (логин)

б) пароль

в) учетная запись

г) ключ

**ВОПРОС** **19.** Совокупность идентификатора и пароля пользователя называется:

а) логин пользователя

б) учетная запись пользователя

в) ключ пользователя

**ВОПРОС** **20.** Присвоение пользователям идентификаторов и проверка предъявляемых идентификаторов по списку присвоенных является:

а) идентификацией пользователя

б) аутентификацией пользователя

в) опознанием пользователя

г) созданием учетной записи пользователя

**ВОПРОС** **21.** Проверка принадлежности пользователю предъявленного им идентификатора является:

а) идентификацией пользователя

б) аутентификацией пользователя

в) регистрацией пользователя

г) созданием учетной записи пользователя

**ВОПРОС** **22.** Факт получения охраняемых сведений злоумышленниками или конкурентами называется:

а) утечкой

б) разглашением

в) взломом

**ВОПРОС** **23.** Умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним, называется:

а) утечкой

б) разглашением

в) взломом

**ВОПРОС** **24.** Бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена, называется:

а) утечкой

б) разглашением

в) взломом

**ВОПРОС** **25.** Атака на ресурс, которая вызывает нарушение корректной работы программного или аппаратного обеспечения, путем создания огромного количества фальшивых запросов на доступ к некоторым ресурсам или путем создания неочевидных препятствий корректной работе называется:

а) «Отказ от обслуживания» (Denial of Service - DoS)

б) срыв стека

в) внедрение на компьютер деструктивных программ

г) перехват передаваемой по сети информации (Sniffing)

д) спуфинг

е) сканирование портов

**ВОПРОС** **26.** Атака, целью которой является трафик локальной сети, называется:

а) «Отказ от обслуживания» (Denial of Service - DoS)

б) срыв стека

в) внедрение на компьютер деструктивных программ

г) снифинг (Sniffing)

д) спуфинг

е) сканирование портов

**ВОПРОС** **27.** Атака, целью которой являются логины и пароли пользователей, атака проходит путем имитации приглашения входа в систему или регистрации для работы с программой, называется:

а) «Отказ от обслуживания» (Denial of Service - DoS)

б) срыв стека

в) внедрение на компьютер деструктивных программ

г) снифинг (Sniffing)

д) спуфинг

е) сканирование портов

**ВОПРОС** **28.** Сетевая атака, целью которой является поиск открытых портов работающих в сети компьютеров, определение типа и версии ОС и ПО, контролирующего открытый порт, используемых на этих компьютерах, называется:

а) «Отказ от обслуживания» (Denial of Service - DoS)

б) срыв стека

в) внедрение на компьютер деструктивных программ

г) снифинг (Sniffing)

д) спуфинг

е) сканирование портов

**ВОПРОС** **29.** Особая категория информации, основной задачей защиты которой является охрана прав человека, который является создателем, называется:

1. коммерческая тайна
2. персональные данные
3. процессуальная тайна
4. авторское или патентное право

**ВОПРОС** **30.** Форма преднамеренного распространения или мнимого разглашения (утечки) неких планов и намерений, которые не отвечают реальным действиям называется:

1. дезинформация
2. легендирование
3. шпионаж

**ВОПРОС** **31.** Долговременная дезинформация и имитация действий, используемых для скрытия от противника реальных планов, намерений и действий называется:

1. дезинформация
2. легендирование
3. шпионаж

**ВОПРОС** **32.** Что из нижеперечисленного оборудования может выступать в качестве технического канала связи?

1. контроллер жесткого диска, передающий электрические импульсы, считанные магниторезистивной головкой с поверхности магнитного носителя, по шлейфу в системную магистраль для копирования в оперативную память
2. инфракрасный светодиод лазерного принтера, посылающий кратковременные вспышки на электризованную поверхность фоточувствительного барабана
3. модулированный по силе тока поток электронов, засвечивающий в определенном порядке пиксели люминофора электронно-лучевой трубки
4. экран компьютерного монитора и глаза пользователя
5. оптический канал связи
6. все варианты могут быть отнесены к техническим каналам связи

**ВОПРОС** **33.** Процесс разведки за объектами на территории другого государства с космических аппаратов является примером утечки информации:

1. визуально-оптического канала
2. электромагнитного канала
3. виброакустического канала
4. материально-вещественного канала

**ВОПРОС**  **34.** Какой канал утечки информации включает в себя весь радиодиапазон от сверхнизких до сверхвысокочастотных волн?

1. визуально-оптический канал
2. электромагнитный канал
3. виброакустический канал
4. материально-вещественный канал

**ВОПРОС** **35.** Процедура опознавания пользователя по предъявленному идентификатору – это …

1. санкционирование
2. авторизация
3. аутентификация
4. идентификация