1. Захист інформації від витоку це діяльність щодо запобігання:  
а) отримання інформації, що захищається зацікавленим суб'єктом з порушенням встановлених правовими документами чи власником, власником інформації прав або правил доступу до інформації, що захищається;  
б) впливу з порушенням встановлених прав і / або правил на зміну інформації, що призводить до спотворення, знищення, копіювання, блокування доступу до інформації, а також до втрати, знищення або збою функціонування носія інформації;  
в) впливу на захищає інформацію помилок користувача інформацією, збою технічних і програмних засобів інформаційних систем, а також природних явищ;  
г) неконтрольованого поширення інформації, що захищається від її розголошення, несанкціонованого доступу;  
д) несанкціонованого доведення захищається інформації до неконтрольованого кількості одержувачів інформації.

2. Захист інформації це:  
а) процес збору, накопичення, обробки, зберігання, розподілу та пошуку інформації;  
б) перетворення інформації, в результаті якого вміст інформації стає незрозумілим для суб'єкта, що не має доступу;  
в) отримання суб'єктом можливості ознайомлення з інформацією, в тому числі за допомогою технічних засобів;  
г) сукупність правил, що регламентують порядок і умови доступу суб'єкта до інформації та її носіїв;  
д) діяльність щодо запобігання витоку інформації, несанкціонованих і ненавмисних дій на неї.  
   
3. Природні загрози безпеки інформації викликані:  
а) діяльністю людини;  
б) помилками при проектуванні АСУ, її елементів або розробці програмного забезпечення;  
в) впливами об'єктивних фізичних процесів або стихійних природних явищ, незалежних від людини;  
г) корисливими устремліннями зловмисників;  
д) помилками при діях персоналу.

4 Штучні загрози безпеки інформації викликані:  
а) діяльністю людини;

б) помилками при проектуванні АСУ, її елементів або розробці програмного забезпечення;  
в) впливами об'єктивних фізичних процесів або стихійних природних явищ, незалежних від людини;  
г) корисливими устремліннями зловмисників;  
д) помилками при діях персоналу.

5 До основних ненавмисним штучним загрозам АСУ відноситься:  
а) фізичне руйнування системи шляхом вибуху, підпалу та т.п .;  
б) перехоплення побічних електромагнітних, акустичних та інших випромінювань пристроїв і ліній зв'язку;  
в) зміна режимів роботи пристроїв або програм, страйк, саботаж персоналу, постановка потужних активних перешкод і т.п .;  
г) читання залишкової інформації з оперативної пам'яті і з зовнішніх запам'ятовуючих пристроїв;  
д) ненавмисні дії, що призводять до часткової або повної відмови системи або руйнування апаратних, програмних, інформаційних ресурсів системи.  
   
6. До стороннім особам порушників інформаційної безпеки належить:  
а) представники конкуруючих організацій.;  
б) персонал, що обслуговує технічні засоби;  
в) технічний персонал, що обслуговує будинок;  
г) користувачі;  
д) співробітники служби безпеки.  
  
7. Спам поширює підроблені повідомлення від імені банків або фінансових компаній, метою яких є збір логінів, паролів і пін-кодів користувачів:  
а) чорний піар;  
б) фішинг;  
в) нігерійські листи;  
г) джерело чуток;  
д) порожні листи.

8. Дублювання повідомлень є загрозою:  
а) доступності;  
б) конфіденційності;  
в) цілісності.

Г) надійності  
д) правильна відповідь відсутня

9. Найнебезпечнішими джерелами внутрішніх загроз є:  
а) некомпетентні керівники;  
б) скривджені співробітники;  
в) цікаві адміністратори.

Г) а і б

Д) правильна відповідь відсутня

10. Вікно небезпеки з'являється, коли:  
а) стає відомо про засоби використання уразливості;  
б) з'являється можливість використовувати уразливість;  
в) встановлюється нове ПЗ.

Г) на початку року  
д) правильна відповідь відсутня

11. У число цілей політики безпеки верхнього рівня входять:  
а) управління ризиками;  
б) визначення відповідальних за інформаційні послуги;  
в) визначення заходів покарання за порушення політики безпеки.  
Г) Ремонт засобів інформаційної інфрастуктури  
д) правильна відповідь відсутня

12. Політика безпеки будується на основі:  
а) загальних уявлень про ІС організації;  
б) вивчення політик родинних організацій;  
в) аналізу ризиків.  
Г) Уявлень керівництва про ІБ  
д) правильна відповідь відсутня

13. У число цілей політики безпеки верхнього рівня входять:  
а) формулювання адміністративних рішень з найважливіших аспектів реалізації програми безпеки;  
б) вибір методів аутентифікації користувачів;  
в) забезпечення бази для дотримання законів і правил.  
Г) Ремонт засобів інформаційної інфрастуктури  
д) правильна відповідь відсутня

14. Ризик є функцією:  
а) розміру можливих збитків;  
б) числа користувачів інформаційної системи;  
в) статутного капіталу організації.  
Г) надійності  
д) правильна відповідь відсутня

15. Перший крок в аналізі загроз - це:  
а) ідентифікація загроз;  
б) аутентифікація загроз;  
в) ліквідація загроз.  
Г) Нейтралізація загроз  
д) правильна відповідь відсутня

16. Оцінка ризиків дозволяє відповісти на наступні питання:  
а) чим ризикує організація, використовуючи інформаційну систему?  
б) чим ризикують користувачі інформаційної системи?  
в) чим ризикують системні адміністратори?

Г) коли це все скінчиться?  
д) правильна відповідь відсутня

17. Для забезпечення інформаційної безпеки мережевих конфігурацій слід керуватися такими принципами:  
а) вироблення і проведення в життя єдиної політики безпеки;  
б) уніфікація апаратно-програмних платформ;  
в) мінімізація числа використовуваних додатків.  
Г) Нейтралізація загроз  
д) правильна відповідь відсутня

18. Екранування може використовуватися для:  
а) попередження порушень І Б;  
б) виявлення порушень;  
в) локалізації наслідків порушень.

Г) фізичної нейтралізації зловмисників  
д) правильна відповідь відсутня

19. Контроль цілісності може використовуватися для:  
а) попередження порушень І Б;  
б) виявлення порушень;  
в) локалізації наслідків порушень.  
Г) Відшкодування збитків  
д) правильна відповідь відсутня

20. Цифровий сертифікат містить:  
а) відкритий ключ користувача;  
б) секретний ключ користувача;  
в) ім'я користувача.  
Г) номер телефону;  
д) правильна відповідь відсутня

21. Екранування на мережевому і транспортному рівнях може забезпечити:  
а) розмежування доступу по мережевих адрес;  
б) вибіркове виконання команд прикладного протоколу;  
в) контроль обсягу даних, переданих по ТСР-з'єднанню.  
Г) Контроль цілісності інформації;  
д) правильна відповідь відсутня