МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЖИТОМИРСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА

Т.А. ВАКАЛЮК

Захист інформації в комп'ютерних системах

навчально-методичний посібник
для студентів напряму 6.040302 Інформатика*

Житомир 2013

УДК 004.056:004.415
ББК 32.973.202-018.2
В14

Затверджено Вченою радою Житомирського державного університету імені Івана Франка протокол №1 від 30.08.2013 р.

Рецензенти:

Сейдаметова З.С. – доктор педагогічних наук, професор

Медведєв М.Г. – кандидат фізико-математичних наук, доцент

В14 **Вакалюк Т.А.**

Захист інформації в комп'ютерних системах. Навчально-методичний посібник для студентів напряму 6.040302 Інформатика*. – Житомир: Вид-во ЖДУ, 2013. – 136 с.

Посібник призначений для використання студентами під керівництвом викладача на лекціях, практичних та лабораторних заняттях. Посібник містить лекційний курс та лабораторний практикум із захисту інформації в комп'ютерних системах. Викладений матеріал відповідає діючій програмі з Захисту інформації в комп'ютерних системах для спеціальності «Інформатика»

Для студентів фізико-математичних спеціальностей вищих педагогічних закладів, вчителів інформатики загальноосвітніх шкіл.

УДК 004.056:004.415
ББК 32.973.202-018.2

ЗМІСТ

Закон України "Про доступ до публічної інформації"

Закон України "Про захист інформації в автоматизованих системах"

Закон України "Про захист інформації в інформаційно-телекомунікаційних системах"

Закон України "Про науково-технічну інформацію"

Закон України "Про державну таємницю"

Концепція національної безпеки України

Концепція технічного захисту інформації в Україні

Положення про порядок здійснення криптографічного захисту інформації в Україні

Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-комунікаційних системах

НД ТЗІ 1.1-003-99 "Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу"

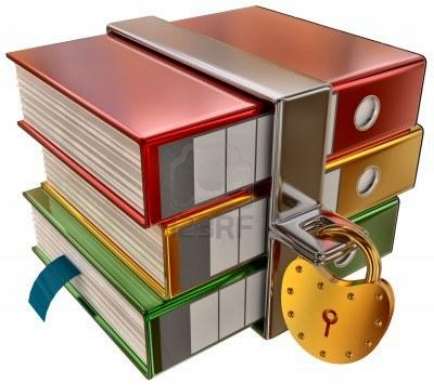
НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу"

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП’ЮТЕРНИХ СИСТЕМАХ

Основні поняття захисту інформації в комп’ютерних системах



По-справжньому безпечною можна вважати лише систему, що виключена, замурована в бетонний корпус, замкнена в приміщенні зі свинцевими стінами й охороняється збройною вартою, але й у цьому випадку сумніви не залишають мене.

Юджин Х. Спаффорд

Мета: ознайомити студентів з основними поняттями захисту інформації в комп'ютерних системах.

Професійна спрямованість: дана лекція є складовою частиною професійної підготовки вчителя інформатики до майбутньої професійної діяльності.

Основні поняття: інформація, інформаційні ресурси, інформатизація, комп’ютерна система, захист інформації, витік інформації, розголошення, несанкціонований доступ, несанкціонований вплив, ненавмисний вплив, конфіденційність, цілісність, доступність, хешування, шифрування, інформаційна безпека.

План лекції:

1. Предмет та об’єкт захисту.
2. Основні поняття.

Обрані методи: лекція-бесіда.

Наочність: схематичні зображення.

Питання по темі для самостійного вивчення:

1. Історичні відомості захисту інформації.

Запитання для самоаналізу та самоперевірки:

1. Інформація, інформаційні ресурси, інформатизація.
2. Комп’ютерна система.
3. Захист інформації, витік інформації, розголошення, несанкціонований доступ, несанкціонований вплив, ненавмисний вплив.
4. Конфіденційність, цілісність, доступність, хешування, шифрування
5. Інформаційна безпека.

Рекомендована література: [4; 3, 345-371; 1, 86-92]

ТЕСТОВІ ЗАВДАННЯ

Загальні відомості із захисту інформації

1. Автором ідеї, завдяки якій значно пізніше виникла технологія створення програмних вірусів, прийнято вважати американського програміста
a) Боба Морріссона
b) Роберта Морріссона
c) Боба Томаса
d) Джона Браннера

2. Чия судова справа була однією з перших справ в обвинуваченні в здійсненні комп'ютерного злочину в США.
a) Боба Морріссона
b) Роберта Морріссона
c) Боба Томаса
d) Джона Браннера

3. Який вчений уперше ввів термін комп'ютерний вірус.
a) Фред Коєн
b) Роберт Морріссон
c) Джон фон Нейман
d) Джон Браннер

4. Перші антивірусні утиліти (1984 рік) були написані...
a) Джон Браннер
b) Роберт Морріссон
c) Анди Хопкинсом
d) Фред Коєн

5. Найпоширенішою антивірусно програмою російського виробництва є:
a) Антивірус Касперського
b) Доктор Web
c) Nod32
d) Avira AntiVir

6. Що на вашу думку може бути складовою частиною інформаційного повідомлення:
а) алфавіт;
б) *знак;*
в) сигнал;
г) *речення;*
д) символ?

7. Основні принципи інформаційних відносин, а саме: гарантованість права на інформацію; відкритість, доступність інформації та свобода її обміну; об'єктивність, вірогідність інформації; повнота і точність інформації; законність одержання, використання, поширення та зберігання інформації сформульовано у:

а) Законі України «Про інформацію»;

б) Державній програмі «Інформаційні та комунікаційні технології в освіті та науці»;

в) Законі України «Про захист інформації в автоматизованих системах»;

г) Законі України «Про Концепцію Національної програми інформатизації».

8. Інформація – це:

а) документовані або публічно оголошені відомості про події та явища, що відбуваються в суспільстві, державі та навколишньому природному середовищі;

б) оброблені дані, що вже передають певний зміст;

в) відомості, які можна накопичувати, зберігати, обробляти у той або інший спосіб, передавати кому-небудь, видозмінювати форму;

г) реляційні бази даних із установленими зв'язками між таблицями.

9. Властивість компонента бути доступним для використання авторизованими суб'єктами в будь-який час – це:

а) доступність компонента(ресурсу);

б) безпека інформаційної системи;

в) цілісність компонента(ресурсу);

г) конфіденційність інформації.

10. Один із найбільш поширених видів комп'ютерних порушень, який полягає в одержанні користувачем доступу до об'єкта, на який у нього немає дозволу згідно з прийнятою в даній системі політикою безпеки – це:

а) несанкціонований доступ;

б) безпека інформаційної системи;

в) цілісність компонента(ресурсу);

г) доступність компонента(ресурсу).

11. У будь-якій захищеній системі передбачені засоби, які використовують за надзвичайних ситуацій, або засоби, які спроможні функціонувати навіть у разі порушення правил запровадженої політики безпеки. Наприклад, у разі несподіваної перевірки роботи системи користувач повинен мати доступ до всіх наборів системи. Звичайно, ці засоби використовуються адміністраторами, операторами, системними програмістами й іншими користувачами, що виконують спеціальні функції. Якщо ці засоби використовуються не за призначенням, то це:

а) незаконне використання привілеїв;

б) безпека інформаційної системи;

в) цілісність компонента(ресурсу);

г) доступність компонента(ресурсу).

12. Якщо зловмисник намагається проникнути в систему для подальшого виконання яких-небудь несанкціонованих дій і для цього він звичайно використовує метод «маскараду», перехоплення або підробки пароля, злому – то це є загроза:

а) інформаційній системі в цілому;

б) об'єктам інформаційної системи;

в) суб'єктам інформаційної системи;

г) каналам передачі даних.

13. Якщо на небезпеку наражаються дані або програми в оперативному запам'ятовуючому пристрої (ОЗП) чи на зовнішніх носіях; самі пристрої системи як зовнішні (дисководи, мережні пристрої, термінали), так і внутрішні (ОЗП, процесор) і злочинний вплив на об'єкти системи звичайно має на меті доступ до їхнього вмісту (порушення конфіденційності або цілісності інформації, що на них зберігається), або порушення їхньої функціональності (наприклад, заповнення всієї ОЗП безглуздою інформацією або завантаження процесора комп'ютера завданням з необмеженим часом виконання) – то це є загроза;

а) об'єктам інформаційної системи;
б) інформаційній системі в цілому;
в) суб'єктам інформаційної системи;
г) каналам передачі даних.

14. Якщо на небезпеку наражаються процеси або підпроцеси користувачів і метою таких атак є прямий вплив на перебіг процесу – його припинення, зміна привілеїв або зворотний вплив – використання зловмисником привілеїв і характеристик іншого процесу зі своєю метою, то це є загроза:

а) суб'єктам інформаційної системи;
б) інформаційній системі в цілому;
в) об'єктам інформаційної системи;
г) каналам передачі даних.

15. Якщо на небезпеку наражаються самі канали або пакети даних, переданих по каналу і вплив на пакети даних може розглядатися як атака на об'єкти мережі; вплив на канали – як специфічний тип атак, характерний для певної мережі, то це є загроза:

а) каналам передачі даних;
б) інформаційній системі в цілому;
в) об'єктам інформаційної системи;
г) суб'єктам інформаційної системи.

16. Чинні у країні закони, укази, нормативні акти, що регламентують правила взаємодії з інформацією обмеженого використання і відповідальність за їх порушення, які відіграють роль стримуючого чинника для потенційних порушень відносять до заходів захисту інформаційних систем:

а) правових;
б) морально-етичних;
в) адміністративних;
г) фізичних.

17. Норми поведінки, що традиційно склалися раніше, виникають або спеціально розробляються в міру поширення ЕОМ та інформаційної системи в країні й у світі. Морально-етичні норми можуть бути неписані (наприклад, чесність) або оформлені у певний перелік правил чи розпоряджень. Ці норми, як правило, не є законодавчо затвердженими, але оскільки їхнє недотримання призводить до падіння престижу організації,

вони є обов'язковими до виконання і їх відносять до заходів захисту інформаційних систем:

а) морально-етичних;
б) правових;
в) адміністративних;
г) фізичних.

18. Заходи організаційного характеру, що регламентують процеси функціонування інформаційної системи, використання її ресурсів, діяльність персоналу і т. ін. Мета цих заходів – найбільшою мірою виключити можливість реалізації загроз безпеці. Такі заходи відносять до:

а) адміністративних;
б) правових;
в) морально-етичних;
г) фізичних.

19. Різного роду механічні, електро- або електронно-механічні пристрої і будови, призначені для створення фізичних перешкод на можливих шляхах проникнення й доступу потенційних порушників до компонентів захисту інформації відносяться до заходів захисту інформаційних систем:

а) фізичних;
б) правових;
в) морально-етичних;
г) адміністративних.

20. Різноманітні електронні й спеціальні програми, що виконують функції захисту. Серед таких функцій відзначимо такі: ідентифікація й аутентифікація (відповідність вимогам на правильність) користувачів або процесів, розмежування і контроль доступу до ресурсів, реєстрація й аналіз подій, криптографічний захист інформації (шифрування даних), резервування ресурсів і компонентів інформаційної системи. Такі заходи відносять до:

а) технічних;
б) правових;
в) морально-етичних;
г) фізичних.

21. Комплекс законів, правил і практичних рекомендацій, на основі яких будується управління, захист і розподіл критичної інформації в системі, – це:

а) політика безпеки;
б) система захисту;
в) безпека інформаційної ситеми;
г) планування захисту інформації.

22. Про наявність вірусу в КС користувач може судити за наступними подіями:

а) поява повідомлень антивірусних засобів про зараження або про передбачуване зараженні;

б) явні прояви присутності вірусу, такі як повідомлення, що видаються на монітор або принтер, звукові ефекти, знищення файлів та інші аналогічні дії, що однозначно вказують на наявність вірусу в КС;

в) неявні прояви зараження, які можуть бути викликані і іншими причинами, наприклад, збоями або відмовами апаратних і програмних засобів КС;

г) наявність у головному меню відповідного повідомлення;

д) повідомлення у Контакті.

Закон України "Про інформацію"

1. Згідно з Законом України «Про інформацію» під захистом інформації розуміють…
   а) перетворення інформації з використанням спеціальних даних з метою приховування змісту інформації, підтвердження її справжності, цілісності;
   б) сукупність методів та засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру;
   в) сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї;
   г) діяльність, спрямовану на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації.

2. Суб'єктами інформаційних відносин є …
   а) фізичні особи, юридичні особи, інформація;
   б) інформація, об'єднання громадян, суб'єкти владних повноважень;
   в) суб'єкти владних повноважень, фізичні особи, юридичні особи;
   г) юридичні особи, інформація, об'єднання громадян.

3. Предметом суспільного інтересу не вважається інформація, яка ….
   а) свідчить про загрозу державному суверенітету;
   б)свідчить про можливість порушення прав людини, введення громадськості в оману;
   в) забезпечує реалізацію конституційних прав;
   г) свідчить про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

4. Які дані відносять до інформації про довкілля?
   а) дані про стан здоров'я та безпеки людей, умови життя людей, стан об'єктів культури і споруд тією мірою, якою на них впливає або може вплинути стан складових довкілля;
   б)відомості про ставлення до окремих осіб, подій, явищ, процесів, фактів тощо;
   в) дані, що дають кількісну характеристику масових явищ та процесів, які відбуваються в економічній, соціальній, культурній та інших сферах життя суспільства;

г) відомості про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення.

5. До інформації з обмеженим доступом не можуть бути віднесені такі відомості…
   а) про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб;
   б) про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою;
   в) про аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей;
   г) про факти порушення прав і свобод людини і громадянина.

6. Що не є джерелом правової інформації?
   а) Конституція України;
   б) архіви різноманітних довідкових інформаційних служб;
   в) ненормативні правові акти;
   г) повідомлення засобів масової інформації, публічні виступи з правових питань.

7. Інформація довідково-енциклопедичного характеру – це…
   а) відомості та/або дані, які розкривають кількісні, якісні та інші характеристики товару;
   б) будь-які відомості та/або дані про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, одержані в ході науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;
   в) документована інформація, що дає кількісну характеристику масових явищ та процесів, які відбуваються в економічній, соціальній, культурній та інших сферах життя суспільства;
   г) систематизовані, документовані, публічно оголошені або іншим чином поширені відомості про суспільне, державне життя та навколишнє природне середовище.

8. До основних видів інформаційної діяльності відносять:
   а) створення, збирання, одержання, видалення;
   б) зберігання, використання, поширення, блокування;
   в) збирання, охорона, зберігання, одержання;
   г) захист, знищення, поширення, створення.

9. Які основні напрями інформаційної діяльності?
   а) політичний, економічний, комп'ютерний, екологічний;
   б) міжнародний, соціальний, політичний, духовний;
   в) духовний, науково-технічний, спортивний, біологічний;

г) екологічний, економічний, міжнародний, суспільний.

10. Які принципи не належать до принципів інформаційних відносин?
а) рівноправність, незалежно від ознак раси, політичних, релігійних та інших переконань, статі, етнічного та соціального походження, майнового стану, місця проживання, мовних або інших ознак, вільне отримання та поширення інформації, крім обмежень, встановлених законом;
б) відкритість, доступність інформації, свобода обміну інформацією, захищеність особи від втручання в її особисте та сімейне життя;
в) достовірність і повнота інформації, свобода вираження поглядів і переконань;
г)гарантованість права на інформацію, правомірність одержання, використання, поширення, зберігання та захисту інформації.

Закон України "Про доступ до публічної інформації"

1. Згідно з Законом України про доступ до публічної інформації, під терміном «публічна інформація» розуміють…
а) систематизовані, документовані, публічно оголошені або іншим чином поширені відомості про суспільне, державне життя та навколишнє природне середовище;
б) будь-які відомості та/або дані про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, одержані в ході науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;
в) відображену та задокументовану будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень;
г) документовану інформацію, що дає кількісну характеристику масових явищ та процесів, які відбуваються в економічній, соціальній, культурній та інших сферах життя суспільства.

2. Яка мета Закону України Про доступ до публічної інформації?
а) забезпечення прозорості та відкритості суб'єктів владних повноважень і створення механізмів реалізації права кожного на доступ до публічної інформації;
б) встановлення загальних правових основ одержання, використання, поширення та зберігання інформації, закріплення права особи на інформацію в усіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначеннястатусу учасників

інформаційних відносин, регулювання доступу до інформації та забезпечення її охорони, захист особи та суспільствавід неправдивої інформації;
в) регулювання відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах;
г) встановлення основ регулювання правових відносин щодо захисту інформації в автоматизованих системах заумови дотримання права власності громадян України і юридичних осібна інформацію та права доступу до неї, права власника інформаціїна її захист, а також встановленого чинним законодавствомобмеження на доступ до інформації.

3. Право на доступ до публічної інформації гарантується:
а) створенням механізму реалізації права на інформацію;
б)обов'язком суб'єктів владних повноважень інформувати громадськість та засоби масової інформації про свою діяльність і прийняті рішення;
в)обов'язком розпорядників інформації надавати та оприлюднювати інформацію, крім випадків, передбачених законом;
г)здійсненням державного і громадського контролю за додержанням законодавства про інформацію.

4. Таємна інформація – це …
а) інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов;
б) інформація, доступ до якої обмежується відповідно до частини другої статті 6 Закону Про доступ до публічної інформації, розголошення якої може завдати шкоди особі, суспільству і державі;
в) відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених Законом Про доступ до публічної інформації;
г) інформація, яка зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

5. Розпорядники інформації, які володіють інформацією про особу, зобов'язані:
а) виправляти неточну та застарілу інформацію про особу самостійно або на вимогу осіб, яких вона стосується, вживати заходів щодо унеможливлення несанкціонованого доступу до неї інших осіб;
б) використовувати її лише з метою та у спосіб, визначений законом, вести облік запитів на інформацію;

в) надавати достовірну, точну та повну інформацію, а також у разі потреби перевіряти правильність та об'єктивність наданої інформації;
г) оприлюднювати інформацію про свою діяльність та прийняті рішення, систематично вести облік документів, що знаходяться в їхньому володінні.

6. Якого контролю за забезпеченням доступу до публічної інформації не існує?
   а) парламентський контроль;
   б) громадський контроль;
   в) державний контроль;
   г) суспільний контроль.

7. Розпорядник інформації має надати відповідь на запит на інформацію не пізніше…
   а) 14 робочих днів з дня отримання запиту;
   б) 2 робочих днів з дня отримання запиту;
   в) 7 робочих днів з дня отримання запиту;
   г) 5 робочих днів з дня отримання запиту.

8. Відповідальність за порушення законодавства про доступ до публічної інформації несуть особи, винні у вчиненні таких порушень…
   а) несвоєчасному наданні інформації, наданні відповіді на запит, наданні інформації на запит;
   б) ненаданні інформації на запит, несвоєчасному наданні інформації, навмисному приховуванні або знищенні інформації чи документів;
   в) ненаданні або не оприлюдненні недостовірної, неточної або неповної інформації, здійсненні реєстрації документів, безпідставній відмові у задоволенні запиту на інформацію;
   г) необґрунтованому віднесенні інформації до інформації з обмеженим доступом, наданні відповіді на запит, наданні інформації на запит.

9. У якому випадку розпорядник інформації має право відмовити в задоволенні запиту?
   а) інформація, що запитується, належить до категорії інформації з обмеженим доступом відповідно до частини другої статті 6 Закону Про доступ до публічної інформації;
   б) особа, яка подала запит на інформацію, оплатила передбачені статтею 21 Закону "Про доступ до публічної інформації" фактичні витрати, пов'язані з копіюванням або друком;
   в) розпорядник інформації володіє і зобов'язаний відповідно до його компетенції, передбаченої законодавством, володіти інформацією, щодо якої зроблено запит;
   г) дотримано вимог до запиту на інформацію, передбачених частиною п'ятою статті 19 Закону Про доступ до публічної інформації.

10. Які рішення, дії чи бездіяльність розпорядників інформації можуть бути оскаржені запитувачем?

а) ненадання недостовірної або неповної інформації;
б) своєчасне надання інформації;
в)ненадання відповіді на запит на інформацію та невиконання розпорядниками обов'язку оприлюднювати інформацію відповідно до статті 15 цього Закону Про доступ до публічної інформації;
г) надання відповіді на запит на інформацію.

Закон України "Про захист інформації в автоматизованих системах"

1. Скільки розділів містить Закон України Про захист інформації в автоматизованих системах?
   а) 4; б) 6; в) 8; г) 10.

2. Яка мета Закону України Про захист інформації в автоматизованих системах?
   а) забезпечення прозорості та відкритості суб'єктів владних повноважень і створення механізмів реалізації права кожного на доступ до публічної інформації;
   б) встановлення загальних правових основ одержання, використання, поширення та зберігання інформації, закріплення права особи на інформацію в усіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначення статусу учасників інформаційних відносин, регулювання доступу до інформації та забезпечення її охорони, захист особи та суспільства від неправдивої інформації;
   в) регулювання відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах;
   г) встановлення основ регулювання правових відносин щодо захисту інформації в автоматизованих системах за умови дотримання права власності громадян України і юридичних осіб на інформацію та права доступу до неї, права власника інформації на її захист, а також встановленого чинним законодавством обмеження на доступ до інформації.

3. Згідно з Законом України Про захист інформації в автоматизованих системах під захистом інформації розуміють…
   а) діяльність, спрямовану на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації;
   б) сукупність методів та засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру;

в) сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї;
г) сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією.

4. Що являється об'єктом захисту відповідно до Закону Про захист інформації в автоматизованих системах?
   а) інформація; в) власники інформації;
   б) користувачі АС; г) користувачі інформації.

5. Згідно 9 статті Закону Про захист інформації в автоматизованих системах (Відносини між власником АС і користувачем АС) власник або розпорядник АС:
   а) повинен забезпечити захист інформації згідно з вимогами і правилами, що обумовлюються угодоюз власником інформації або уповноваженою ним особою, та зобов'язаний повідомити його про всі факти порушення її захисту;
   б) не несе відповідальності за шкоду, заподіяну власнику інформації, якщо при цьому не було порушено встановлені власником інформації правила її захисту;
   в) повинен інформувати власника і користувача інформації про властивості методів обробки інформації та межі їх використання, а власник і користувач інформації повинні підтвердити свою згоду на застосування пропонованих методів обробки та відсутність претензій;
   г) визначає користувачів належної йому інформації та встановлює їх повноваження.

6. Яким шляхом здійснюється захист інформації в АС?
   а) використання засобів обчислювальної техніки, програмного забезпечення, засобів зв'язку і АС в цілому, засобів захисту інформації, які відповідають встановленим вимогам щодо захисту інформації (мають відповідний сертифікат);
   б) перетворення інформації з використанням спеціальних(ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо;
   в) проведення єдиної технічної політики щодо захисту інформації;
   г) створення відповідних структур для захисту інформації в АС.

7. Яку відповідальність не несуть особи, винні в порушенні порядку і правил захисту оброблюваної в АС інформації?
   а)кримінальну; в)юридичну;
   б)матеріальну; г)дисциплінарну.

8. Згідно з Законом України Про захист інформації в автоматизованих системах під втратою інформації розуміють…
   а) дії, наслідком яких є припинення доступу до інформації;
   б) дію, внаслідок якої інформація в АС перестає існувати для фізичних або юридичних осіб, які мають право власності на неї в повному чи обмеженому обсязі;
   в) дії або обставини, які призводять до спотворення процесу обробки інформації.
   г) навмисні дії, що призводять до перекручення інформації, яка повинна оброблятися або зберігатися в
   АС.

9. Кому належить інформація, яка створена як вторинна в процесі обробки в АС, коли відсутня угода між власником вхідної інформації і користувачем АС?
   а)користувачу інформації; в)власнику вхідної інформації;
   б)власнику АС; г)користувачу АС.

Закон України "Про захист інформації в інформаційно-телекомунікаційних системах"

1. Скільки розділів містить Закон України Про захист інформації в інформаційно-телекомунікаційних системах?
   а) 4; в) 8;
   б) 6; г) немає правильної відповіді.

2. Яка мета Закону України Про захист інформації в інформаційно-телекомунікаційних системах?
   а) забезпечення прозорості та відкритості суб'єктів владних повноважень і створення механізмів реалізації права кожного на доступ до публічної інформації;
   б) встановлення загальних правових основ одержання, використання, поширення та зберігання інформації, закріплення права особи на інформацію в усіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначення статусу учасників інформаційних відносин, регулювання доступу до інформації та забезпечення її охорони, захист особи та суспільства від неправдивої інформації;
   в) регулювання відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах;
   г) встановлення основ регулювання правових відносин щодо захисту інформації в автоматизованих системах за умови дотримання права власності громадян України і юридичних осіб на інформацію та права доступу до неї, права власника інформації на її захист, а також

встановленого чинним законодавством обмеження на доступ до інформації.

3. Згідно з Законом України Про захист інформації в інформаційно-телекомунікаційних системах під захистом інформації в системі розуміють…
   а) діяльність, спрямовану на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації;
   б) діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі;
   в) сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї;
   г) сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією.

4. Що не є суб'єктом відносин, пов'язаних із захистом інформації в системах?
   а) інформація;
   б) спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації і підпорядковані йому регіональні органи;
   в) власники інформації;
   г) користувачі.

5. Ким визначається порядок доступу до інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, перелік користувачів та їх повноваження стосовно цієї інформації?
   а) власником інформації;
   б) законодавством;
   в) спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації;
   г) власником системи.

6. Хто надає користувачеві відомості про правила і режим роботи системи та забезпечує йому доступ до інформації в системі відповідно до визначеного порядку доступу?
   а) спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації;
   б) законодавств;
   в) користувач;
   г) власник системи.

7. Відповідальність за забезпечення захисту інформації в системі покладається на…
   а) власника інформації; в) користувача;
   б)законодавство; г) власника системи.

8. Ким встановлюються особливості захисту інформації в системах, які забезпечують банківську діяльність?
   а) Кабінетом Міністрів України;
   б) законодавством;
   в) Національним банком України;
   г) спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації.

9. Хто визначає вимоги та порядок створення комплексної системи захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом?
   а) Кабінет Міністрів України;
   б) законодавство;
   в) Національний банк України;
   г) спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації.

Закон України "Про науково-технічну інформацію"

1. Даний Закон визначає:
   a) основи державної політики в галузі соціально-технічної інформації, порядок її формування і реалізація в інтересах політичного, економічного і соціального прогресу;
   b) основи державної політики в галузі наукової інформації, порядок її формування і реалізація в інтересах політичного, економічного і соціального прогресу;
   c) основи державної політики в галузі науково-технічної інформації, порядок її формування і реалізація в інтересах науково-технічного, економічного і соціального прогресу;
   d) основи державної політики в галузі науково-соціальної інформації, порядок її формування і реалізація в інтересах економічного і соціального прогресу.

2. Метою даного Закону є
   a) створення в Україні правової бази для одержання та використання наукової інформації;
   b) створення в Україні правової бази для одержання та використання науково-технічної інформації;

c) створення в Україні правової бази для одержання та використання технічної та технологічної інформації;
d) створення в Україні правової бази для одержання та використання забороненої інформації.

3. Даний Закон включає в себе
   a) 5 розділів (16 статей);
   b) 6 розділів (23 статті);
   c) 3 розділи (15 статей);
   d) 7 розділів (30 статей).

4. У цьому Законі науково-технічна інформація вживається у значенні:
   a) будь-які відомості та/або дані про досягнення науки, техніки і виробництва, одержані в ході соціальної, політичної та громадської діяльності, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;
   b) будь-які відомості та/або дані про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, одержані в ході науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;
   c) будь-які відомості та/або дані про вітчизняні та зарубіжні досягнення науки, одержані в ході інтегрованої та громадської діяльності, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;
   d) правильної відповіді немає.

5. У цьому Законі інформаційний ринок вживається у значенні:
   a) система економічних, організаційних і правових відносин щодо продажу і купівлі соціальних ресурсів;
   b) система економічних, організаційних і правових відносин щодо продажу і купівлі інформаційних ресурсів, технологій, продукції та послуг;
   c) система економічних та соціальних відносин щодо продажу і купівлі інформаційних ресурсів, технологій, продукції та послуг;
   d) правильної відповіді немає.

6. Об'єктом відносин у сфері науково-технічної інформації є
   a) зарубіжна соціальна інформація;
   b) вітчизняна технічна інформація;
   c) вітчизняна і зарубіжна науково-технічна інформація;
   d) вітчизняна і зарубіжна соціальна інформація.

7. Суб'єктами відносин, що регулюються цим Законом, є державні органи, органи місцевого і регіонального самоврядування, юридичні особи та громадяни України, міжнародні організації, іноземні юридичні особи і громадяни та особи без громадянства

a) державні органи, органи місцевого і регіонального самоврядування;
b) державні органи, органи місцевого і регіонального самоврядування, юридичні особи та громадяни України;
c) державні органи, органи місцевого і регіонального самоврядування, юридичні особи та громадяни України, міжнародні організації, іноземні юридичні особи і громадяни та особи без громадянства;
d) державні органи і громадяни та особи без громадянства.

8. Вкажіть правильні ланцюги відносин між власником інформації, споживачем і посередником:
   a) споживач науково-технічної інформації несе відповідальність за дотримання прав власника цієї інформації;
   b) відносини між власником і посередником регулюються договором;
   c) власник здійснює своє право щодо науково-технічної інформації самостійно або через посередника;
   d) власник не здійснює свого права щодо науково-технічної інформації самостійно;
   e) відносини між власником і посередником не регулюються.

9. Основною метою національної системи науково-технічної інформації є
   a) збереження науково-технічної інформації;
   b) перевірка правильності відправлення науково-технічної інформації;
   c) задоволення потреб громадян, юридичних осіб і держави в науково-технічній інформації;
   d) перевірка правильності доставки науково-технічної інформації.

10. Інформаційна продукція та послуги органів науково-технічної інформації, а також підприємств, установ, організацій, окремих громадян, які здійснюють науково-інформаційну діяльність, можуть бути
    a) суб'єктами товарних відносин, що регулюються чинним законодавством;
    b) об'єктами товарних відносин, що регулюються чинним законодавством;
    c) суб’єктами та об'єктами товарних відносин, що регулюються чинним законодавством;
    d) правильної відповіді немає.

11. Як називається основний документ, що регламентує відносини між виробником і споживачем інформації
    a) угода;
    b) договір;
    c) контракт;
    d) заява.

12. Чи можуть інвестувати розвиток сфери науково-технічної інформації України іноземні юридичні та фізичні особи, а також особи без громадянства
    a) так;
    b) ні;
    c) певною мірою.

Закон України "Про державну таємницю"

1. Даний Закон регулює
   a) соціальні відносини, пов'язані з віднесенням інформації до державної таємниці та охороною державної таємниці з метою захисту національної безпеки України;
   b) суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України;
   c) політичні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України.

2. Даний Закон включає в себе
   a) 5 розділів (16 статей);
   b) 6 розділів (23 статті);
   c) 4 розділи (20 статей);
   d) 7 розділів (30 статей).

3. У цьому Законі гриф секретності вживається у значенні:
   a) реквізит флеш носія секретної інформації, що засвідчує ступінь захищеності даної інформації;
   b) реквізит інтегрального носія секретної інформації, що засвідчує ступінь передаваності даної інформації;
   c) реквізит матеріального носія секретної інформації, що засвідчує ступінь секретності даної інформації.

4. Які є ступені секретності інформації?
   a) "особливої важливості", "цілком таємно", "таємно";
   b) "важливо", "таємно", "не таємно";
   c) "особливої важливості", "особливої таємності", "таємно";
   d) "важливо", "цілком таємно", "таємно".

5. Хто видає укази та розпорядження з питань охорони державної таємниці, віднесених цим Законом та іншими законами до його повноважень
   a) Кабінет Міністрів;
   b) Президент;
   c) Верховна Рада;
   d) Рада національної безпеки і оборони.

6. Хто координує та контролює діяльність органів виконавчої влади у сфері охорони державної таємниці
   a) Кабінет Міністрів;
   b) Президент;
   c) Верховна Рада;
   d) Рада національної безпеки і оборони.

7. До державної таємниці у порядку, встановленому цим Законом, відноситься інформація:
   a) у сфері оборони;
   b) у сфері економіки, науки і техніки;
   c) у сфері зовнішніх відносин;
   d) у сфері державної безпеки та охорони правопорядку;
   e) всі перелічені відповіді.

8. Ким здійснюється віднесення інформації до державної таємниці
   a) державним експертом;
   b) президентом країни;
   c) Верховною Радою;
   d) Кабінетом Міністрів.

9. З якого часу інформація вважається державною таємницею?
   a) з часу опублікування відповідного закону;
   b) з часу опублікування Зводу відомостей;
   c) з часу, коли її визнали таємною;
   d) всі відповіді вірні.

10. Реквізити кожного матеріального носія секретної інформації складаються із:
    a) грифа секретності;
    b) номера примірника;
    c) статті Зводу відомостей, що становлять державну таємницю, на підставі якої здійснюється засекречення;
    d) найменування посади та підпису особи, яка надала гриф секретності;
    e) всі перелічені відповіді вірні.

11. Перебіг строку засекречування матеріальних носіїв інформації починається з часу
    a) надання їм грифу секретності;
    b) з часу опублікування Зводу відомостей;
    c) з часу опублікування відповідного закону.

Концепція національної безпеки України

1. Цим документом закладаються основи
   a) концептуалізації державної політики України;
   b) концептуалізації державної політики національної безпеки;
   c) концептуалізації державної певного регіону.
2. Спрямування діяльності держави, визначення форм, завдань, змісту її діяльності – це
   a) внутрішня політика;
   b) зовнішня політика;
   c) державна політика.

3. Визначальні потреби держави, які співвідносяться з її базовими цінностями і виражаються у затвердженому Верховною Радою комплексі цілей називають
   a) національними;
   b) суспільними;
   c) політичними;
   d) індивідуальними.

4. Що таке рівень захищеності життєво-важливих інтересів, прав і свобод особи, життєво-важливих інтересів суспільства, держави та її довкілля від зовнішніх та внутрішніх загроз?
   a) державна безпека;
   b) національна безпека;
   c) політична безпека.

5. Головним інтегральним критерієм ефективності державної політики національної безпеки є
   a) досягнута захищеність прав і свобод особи від зовнішніх та внутрішніх загроз;
   b) досягнута захищеність прав і свобод особи від зовнішніх загроз;
   c) досягнута захищеність прав і свобод особи від внутрішніх загроз.

6. В формуванні і реалізації державної політики національної безпеки беруть участь
   a) Президент України;
   b) Верховна Рада України;
   c) Кабінет Міністрів України;
   d) Рада національної безпеки і оборони України;
   e) Центральні та місцеві органи виконавчої влади;
   f) всі перелічені пункти вірні.

7. Концептуальний документ вищого рівня
   a) Концепція (Основи) національної безпеки України;
   b) Стратегія національної безпеки України;
   c) стратегії (доктрини) по складових (аспектах) державної політики.

8. Концептуальні документи першого рівня
   a) Концепція (Основи) національної безпеки України;
   b) Стратегія національної безпеки України;
   c) стратегії (доктрини) по складових (аспектах) державної політики.

9. Концептуальні документи другого рівня
   a) Концепція (Основи) національної безпеки України;
   b) Стратегія національної безпеки України;
   c) стратегії (доктрини) по складових (аспектах) державної політики.

10. Національні інтереси України складаються з наступних груп:
    a) Національні інтереси загальнодержавного характеру;

b) Національні інтереси, що відображають внутрішні відносини в державі;
c) Національні інтереси, що відображають зовнішні відносини держави;
d) Національні інтереси, що стосуються оборони держави та діяльності її силових органів;
e) Всі перелічені відповіді вірні.

Концепція технічного захисту інформації в Україні

1. Ця Концепція визначає основи державної політики у сфері захисту інформації
a) науково-технічними заходами;
b) інженерно-технічними заходами;
c) інженерними заходами;
d) іншими заходами.

2. ТЗІ – це діяльність, спрямована на
a) забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності інформації з обмеженим доступом, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави;
b) забезпечення науково-технічними заходами порядку доступу, цілісності та доступності інформації з обмеженим доступом, а також цілісності;
c) забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності інформації з необмеженим доступом.

3. Система ТЗІ – це
a) сукупність об'єктів, об'єднаних цілями та завданнями захисту інформації інженерно-технічними заходами, нормативно-правова база;
b) сукупність суб'єктів, об'єднаних цілями та завданнями захисту інформації інженерно-технічними заходами, нормативно-правова та матеріально-технічна база.

4. Основними напрямами державної політики у сфері ТЗІ є
a) нормативно-правове забезпечення;
b) організаційне забезпечення;
c) науково-технічна та виробнича діяльність;
d) удосконалення чинних та розроблення нових нормативних документів з питань ТЗІ;
e) всі перелічені відповіді вірні.

5. Правову основу забезпечення ТЗІ в Україні становлять:
a) Конституція України ,
b) Концепція національної безпеки України ,

c) Закони України "Про інформацію",
d) "Про доступ до публічної інформації",
e) "Про захист інформації в інформаційно-телекомунікаційних системах",
f) всі перелічені відповіді вірні.

Положення про порядок здійснення криптографічного захисту інформації в Україні

1. Яку кількість підпунктів містить ***Положення про порядок здійснення криптографічного захисту інформації в Україні***:
А) 15; Б) 14; В) 16.

2. Указом Президента України від 22 травня 1998 року N 505/98 було затверджено:
А) Положення про порядок здійснення криптографічного захисту інформації в Україні;
Б) Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-комунікаційних системах;
В) НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу;
Г) НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу.

3. Чи містить ***Положення про порядок здійснення криптографічного захисту інформації в Україні*** поняття «криптографічна інформація»:
А) так; Б) ні.

4. Чи містить ***Положення про порядок здійснення криптографічного захисту інформації в Україні*** поняття «криптографічна система»:
А) так; Б) ні.

5. Для криптографічного захисту інформації, що становить державну таємницю, та службової інформації, створеної на замовлення державних органів або яка є власністю держави, використовуються:
А) криптографічні сертифікати; В) криптографічні методи;
Б) криптографічні системи; Г) криптографічні архіви.

Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-комунікаційних системах

1. Яку кількість підпунктів містить постанова про ***Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-комунікаційних системах***:
А) 26; Б) 25; В) 27.

2. Кабінет міністрів України від 29 березня 2006 р. N 373 затвердив:
А) Положення про порядок здійснення криптографічного захисту інформації в Україні;
Б) Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-комунікаційних системах;
В) НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу;
Г) НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

3. Чи містить постанова про ***Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-комунікаційних системах*** поняття «аутентифікація»:
А) так; Б) ні.

4. Чи містить постанова ***Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-комунікаційних системах*** поняття «автентифікація»:
А) так; Б) ні.

5. Згідно постанови про ***Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-комунікаційних системах*** відкрита інформація під час обробки в системі повинна зберігати:
А) надійність; В) цілісність;
Б) правильність; Г) конфіденційність.

6. Згідно постанови про ***Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-комунікаційних системах*** порядок підключення систем, в яких обробляється службова і таємна інформація, до глобальних мереж передачі даних визначається;
А) законодавством;
Б) виконавчою владою;

В) постановою про Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-комунікаційних системах;
Г) інша відповідь.

НД ТЗІ 1.1-003-99 "Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу"

1. Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від “ 28 ” квітня 1999 р. № 22:
А) Положення про порядок здійснення криптографічного захисту інформації в Україні;
Б) Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-комунікаційних системах;
В) НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу;
Г) НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу.

2. Згідно із НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу ***поняття «обчислювальна система» – це:***
А) сукупність програмних та апаратних засобів, призначених для обробки інформації;
Б) організаційно-технічна система, що реалізує інформаційну технологію і об’єднує операційні системи, фізичне середовище, персонал і інформацію, яка обробляється;
В) сукупність програмно-апаратних засобів, яка подана для оцінки.
3. Згідно із НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу ***поняття «автоматизована система» – це:***
А) сукупність програмних та апаратних засобів, призначених для обробки інформації;
Б) організаційно-технічна система, що реалізує інформаційну технологію і об’єднує операційні системи, фізичне середовище, персонал і інформацію, яка обробляється;
В) сукупність програмно-апаратних засобів, яка подана для оцінки.

4. Згідно із НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу ***поняття «комп’ютерна система» – це:***

А) сукупність програмних та апаратних засобів, призначених для обробки інформації;
Б) організаційно-технічна система, що реалізує інформаційну технологію і об'єднує операційні системи, фізичне середовище, персонал і інформацію, яка обробляється;
В) сукупність програмно-апаратних засобів, яка подана для оцінки.

5. Згідно із НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу ***поняття «об'єкт комп'ютерної системи» – це:***
А) виконувана в даний момент програма, яка повністю характеризується своїм контекстом (поточним станом регістрів обчислювальної системи, адресним простором, повноваженнями тощо);
Б) елемент ресурсу комп'ютерної системи, що знаходиться під керуванням КЗС(комплекс засобів захисту) і характеризується певними атрибутами і поводженням;
В) подання фізичного користувача в комп'ютерну систему, що створюється в процесі входження користувача в систему і повністю характеризується своїм контекстом (псевдонімом, ідентифікаційним кодом, повноваженнями тощо).

6. Згідно із НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу ***поняття «об'єкт-процес» – це:***
А) виконувана в даний момент програма, яка повністю характеризується своїм контекстом (поточним станом регістрів обчислювальної системи, адресним простором, повноваженнями тощо);
Б) елемент ресурсу комп'ютерної системи, що знаходиться під керуванням КЗС(комплекс засобів захисту) і характеризується певними атрибутами і поводженням;
В) подання фізичного користувача в комп'ютерну систему, що створюється в процесі входження користувача в систему і повністю характеризується своїм контекстом (псевдонімом, ідентифікаційним кодом, повноваженнями і т. ін.).

7. Згідно із НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу ***поняття «об'єкт-користувач» – це:***
А) виконувана в даний момент програма, яка повністю характеризується своїм контекстом (поточним станом регістрів обчислювальної системи, адресним простором, повноваженнями тощо);
Б) елемент ресурсу комп'ютерної системи, що знаходиться під керуванням КЗС(комплекс засобів захисту) і характеризується певними атрибутами і поводженням;
В) подання фізичного користувача в комп'ютерну систему, що

створюється в процесі входження користувача в систему і повністю характеризується своїм контекстом (псевдонімом, ідентифікаційним кодом, повноваженнями і т. ін.).

НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу"

1. Згідно ***НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу*** в процесі оцінки спроможності комп'ютерної системи забезпечувати захист оброблюваної інформації від несанкціонованого доступу розглядаються вимоги виду:

А) вимоги до безпеки захисту;
Б) вимоги до систем захисту;
В) вимоги до функцій захисту;
Г) вимоги до гарантій.

2. Згідно ***НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу*** функціональні критерії розбиті на такі групи:

А) конфіденційність, цілісність;
Б) конфіденційність, достовірність;
В) доступність, завершеність;
Г) доступність, спостереженість.

3. Згідно ***НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу*** крім функціональних критеріїв, що дозволяють оцінити наявність послуг безпеки в комп'ютерній системі, цей документ містить критерії:

А) законів; Б) гарантій; В) санкцій; Г) завдань.

4. Згідно ***НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу*** поняття «відкат» означає:

А) завжди доступна автоматизована послуга;
Б) завжди доступна гарантована послуга;
В) завжди доступна надійна послуга.

5. Згідно ***НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу*** стійкість до відмов гарантує:

А) незалежність комп’ютерної системи;
Б) надійність комп’ютерної системи;
В) доступність комп’ютерній системі.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Алексеенко В.Н., Сокольский Б.В. Система защиты коммерческих объектов. Технические средства защиты. Практическое пособие для предпринимателей и руководителей служб безопасности. М., 1992. – 94 с.
2. Барсуков В.С. Обеспечение информационной безопасности. – М: ТЭК, 1996.
3. Безруков Н.Н. Компьютерная вирусология: Справ, руководство. – М.: УРЕ, 1991.-416 с.
4. Вернигоров Н.С. Нелинейный локатор – эффективное средство обеспечения безопасности в области утечки информации // Защита информации. Конфидент. – 1996. -№ 1.
5. Герасименко ВА Защита информации в автоматизированных системах обработки данных: В 2 кн. М.: Энергоатомиздат, 1994.
6. Грушо А.А.. Тимонина Е.Е. Теоретические основы защиты информации. -М: Издательство Агентства «Яхтсмен». 1996. – 192 с. '
7. Информационно-безопасные системы. Анализ проблемы: Учеб. пособие / Алешин И.В. и др.: Под ред. В.Н. Козлова – СПб.: Издательство С-Петербургского гос. техн. университета, 1996. – 69 с.
8. Кнут Д. Искусство программирования для ЭВМ. -М.: Мир, 1976. -Т.2.
9. Мамиконов А.Г., Кульба В.В.,Шелков А.Б. Достоверность, защита и резервирование информации в АСУ. – Энергоатомиздат, 1986. – 304 с.
10. Маркин А.В. Безопасность излучений и наводок от средств электронно-вычислительной техники: домыслы и реальность. Защита информации. Конфидент. – 1994. – №2. – С.49-57.
11. Мельников В.В. Защита информации в компьютерных системах. – М: Финансы и статистика; Электронинформ, 1997. – 368 с.
12. Пилюгин П.Л. Общие вопросы зашиты вычислительных систем и особенности защиты персональных компьютеров: Курс лекций. – М.: ИКСИ, 1997. – 84 с.
13. Расторгуев СП. Программные методы защиты в компьютерных сетях. – М.: «Яхтсмен», 1993.-188 с.
14. Спесивцев А.В., Вегнер В.А., Крутяков А.Ю. и др. Защита информации в персональных ЭВМ. – М.: Радио и связь; МП «Веста», 1992. – 192 с.
15. Фоменков Г.В. и др. Методы и средства обеспечения безопасности в сети Интернет: Научно-практическое пособие. -М.: ИКСИ, 1997. – 112 с.
16. Фролов А.В., Фролов Г.В. Осторожно: компьютерные вирусы. -М.:ДИАЛОГ-МИФИ,1996. – 256 с.
17. Хоффман Л.Дж. Современные методы защиты информации / Пер. с англ. -М: Сов. радио, 1980.
18. Щербаков А.Ю. Защита от копирования. – М.: Эдэль, 1992.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

NIST – Національний Інститут Стандартів і Технологій США

ВЗП – внутрішній запам’ятовуючий пристрій

ЕОМ – електронно-обчислювальна машина

ЕОТ – електронна обчислювальна техніка

ЗЗП – зовнішній запам’ятовуючий пристрій

КПП – контрольно-пропускні пункти

КС – комп'ютерна система

НСДІ – несанкціонований доступ до інформації

ОП – оперативна пам'ять

ОС – операційні системи

ОСс – обчислювальні системи

ПЕВІН – побічні електромагнітні випромінювання і наведення

ПЕМВН – побічні електромагнітні випромінювання і наведення

ПЕОМ – персональна електронно-обчислювальна машина

ПОКВ – пристрій обробки і комутації відеоінформації

ПРІ – пристрої реєстрації інформації

СОО – система охорони об'єкта

СРД – системи розмежування доступу

ТЗ – технічні засоби

ТСВ – телевізійні системи відеоконтролю

ДЛЯ НОТАТОК

Навчально-методичне видання

ВАКАЛЮК Тетяна Анатоліївна

ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ

*Навчально-методичний посібник для студентів напряму 6.040302 Інформатика**

Надруковано з оригінал-макета автора

Підписано до друку 30.08.13. Формат 60х90/16. Папір офсетний.
Гарнітура Times New Roman. Друк різографічний.
Ум. друк. арк. 8,0. Обл. вид. арк. 7,1. Наклад 300. Зам. 725.
Видавець і виготовлювач
Видавництво Житомирського державного університету імені Івана Франка
м. Житомир, вул. Велика Бердичівська, 40
Свідоцтво суб’єкта видавничої справи:
серія ЖТ №10 від 07.12.04 р.
електронна пошта (E-mail): zu@zu.edu.ua