Кафедра комп'ютерної інженерії та електроніки

Назва дисципліни – Захист інформації в комп’ютерних системах

Викладач: Павлюк Мирослав Федорович

1. Теоретичні основи захисту інформації в комп’ютерних системах.
2. Сутність проблеми та завдання захисту інформації в інформаційних та телекомунікаційних мережах.
3. Проблеми захисту інформації в комп`ютерних мережах.
4. Захист об’єктів інформації, інформаційних систем підприємств, установ та організацій від протиправних посягань.
5. Захист інформації та використання інформаційних технологій в інтелектуальній власності.
6. Організація комп’ютерної безпеки та захисту інформації.

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; c) контракт;
    b) договір; 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.

СУТНІСТЬ ПРОБЛЕМИ ТА ЗАВДАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ ТА ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Нечушкін М.П., Зінченко М.О.
НЦЗІ ВІТІ ДУТ

Широке застосування комп'ютерних технологій в автоматизованих системах обробки інформації та управління призвело до загострення проблеми захисту інформації, що циркулює в комп'ютерних системах, від несанкціонованого доступу. Захист інформації в комп'ютерних системах має ряд специфічних особливостей, пов'язаних з тим, що інформація не є жорстко пов'язаною з носієм, може легко і швидко копіюватись та передаватись через канали зв'язку. Відома дуже велика кількість загроз інформації, які можуть бути реалізовані як з боку зовнішніх, так і з боку внутрішніх порушників режиму таємності.

У сфері захисту інформації та комп'ютерної безпеки в цілому найбільш актуальними є три групи проблем:

порушення грифу обмеження доступу;

порушення цілісності інформації;

порушення дієздатності інформаційно-обчислювальних систем.

Захист інформації перетворюється у найважливішу проблему державної безпеки, коли мова йде про державну, дипломатичну, військову, промислову, медичну, фінансову та іншу таємну інформацію. Величезні масиви такої інформації зберігаються в електронних архівах, оброблюються в інформаційних системах та передаються через телекомунікаційні мережі. Основні властивості цієї інформації – конфіденційність та цілісність, повинні підтримуватись законодавчо, юридично, а також організаційними, технічними та програмними методами.

Гриф обмеження доступу інформації передбачає введення певних обмежень на коло осіб, що мають доступ до даної інформації. Ступінь обмеження доступу виражається деякою встановленою характеристикою (особливо важливо, цілком таємно, таємно, для службового користування, не для друку тощо), яка суб'єктивно визначається володарем інформації в залежності від змісту відомостей, які не підлягають розголошенню, призначені обмеженому колу осіб, є таємницею. Звичайно, встановлена ступінь таємності інформації повинна зберігатись при її обробці в інформаційних системах та при передачі через телекомунікаційні мережі.

Другою важливою властивістю інформації є її цілісність. Інформація цілісна, якщо вона в будь-який момент часу правильно (адекватно) відображає свою предметну галузь. Цілісність інформації в інформаційних системах забезпечується своєчасним вводом в неї достовірної (вірної) інформації, підтвердженням істинності інформації, захистом від спотворень та руйнувань (видалення).

Несанкціонований доступ до інформації осіб, що не мають до неї допуску, навмисні та ненавмисні помилки операторів, користувачів та програм, невірні зміни інформації внаслідок збоїв обладнання призводять до порушення цих найважливіших властивостей інформації та роблять її непридатною і навіть небезпечною. Її використання може призвести до матеріального та/чи морального збитку, тому створення системи захисту інформації стає актуальним завданням. Під

безпекою інформації розуміють захищеність інформації від небажаного її розголошення (порушення конфіденційності), спотворення (порушення цілісності), втрати чи зниження ступеня доступності інформації, а також незаконного її тиражування.

Безпека інформації в інформаційній системі чи телекомунікаційній мережі забезпечується здатністю цієї системи зберігати таємність інформації при її введенні, виведенні, передаванні, обробці та зберіганні, а також протистояти її руйнуванню, крадіжкам чи спотворенню. Безпека інформації забезпечується шляхом організації допуску до неї, захисту її від перехвату, спотворення чи введення помилкової інформації. З цією метою застосовуються фізичні, технічні, апаратні, програмно-апаратні та програмні засоби захисту. Останні посідають центральне місце в системі забезпечення безпеки інформації в інформаційних системах та телекомунікаційних мережах.

Завдання забезпечення безпеки інформації:

- захист інформації в каналах зв’язку та базах даних криптографічними методами;
- підтвердження справжності об’єктів даних та користувачів (аутентифікація сторін, що встановлюють зв'язок);
- виявлення порушень цілісності об’єктів даних;
- забезпечення захисту технічних засобів та приміщень, в яких ведеться обробка конфіденційної інформації, від витоку через побічні канали і від можливо вбудованих в них електронних пристроїв знімання інформації;
- забезпечення захисту програмних продуктів та засобів обчислювальної техніки від внесення в них програмних вірусів та закладок;
- захист від несанкціонованих дій через канал зв’язку від осіб, що не допущені до засобів шифрування, але що переслідують цілі компрометації таємної інформації і дезорганізації роботи абонентських пунктів;
- організаційно-технічні заходи, спрямовані на забезпечення збереження інформації з обмеженим доступом;
- виконання вимог з кібербезпеки в інформаційних мережах.

УДК 004.056.53

Бакін Д.С.
Кіровоградський національний технічний університет

Проблеми захисту інформації в комп`ютерних мережах

Широке застосування комп'ютерних технологій в автоматизованих системах обробки інформації та управління призвело до загострення проблеми захисту інформації, що циркулює в комп'ютерних системах, від несанкціонованого доступу. Захист інформації в комп'ютерних системах має низку специфічних особливостей, пов'язаних з тим, що інформація не є жорстко пов'язаною з носієм, може легко і швидко копіюватися і передаватися по каналах зв'язку. Відома дуже велика кількість загроз інформації, які можуть бути реалізовані як з боку внутрішніх порушників , так і зовнішніх.

Радикальне вирішення проблем захисту електронної інформації може бути отримано тільки на базі використання криптографічних методів, які дозволяють вирішувати найважливіші проблеми захищеної автоматизованої обробки та передачі даних. При цьому сучасні швидкісні методи криптографічного перетворення дозволяють зберегти початкову продуктивність автоматизованих систем. Криптографічні перетворення даних є найбільш ефективним засобом забезпечення конфіденційності даних, їхньої цілісності і справжності. Тільки їх використання в сукупності з необхідними технічними та організаційними заходами можуть забезпечити захист від широкого спектру потенційних загроз.

Основні проблеми, що виникають з безпекою передачі інформації в комп'ютерних мережах, можна поділити на такі :

— Перехоплення інформації - цілісність інформації зберігається, але її конфіденційність порушена;

— Модифікація інформації - вихідне повідомлення змінюється або повністю підміняється іншим і надсилається адресату;

— Підміна авторства інформації. Дана проблема може мати серйозні наслідки. Наприклад, хтось може надіслати листа від чужого імені (цей вид обману прийнято називати спуфінгом) або Web-сервер може прикидатися електронним магазином, приймати замовлення, номери кредитних карт, але не висилати ніяких товарів.

Потреби сучасної практичної інформатики призвели до виникнення нетрадиційних завдань захисту електронної інформації, однією з яких є автентифікація електронної інформації в умовах, коли сторони що обмінюються інформацією не довіряють одна одній. Ця проблема

пов'язана зі створенням систем електронного цифрового підпису. Технічною основою переходу в інформаційне суспільство є сучасні мікроелектронні технології, які забезпечують безперервне зростання якості засобів обчислювальної техніки і служать базою для збереження основних тенденцій її розвитку - мініатюризації, зниження електроспоживання, збільшення обсягу оперативної пам'яті (ОП) і місткості вбудованих і змінних накопичувачів, зростання продуктивності і надійності, розширення сфер і масштабів застосування. Дані тенденції розвитку засобів обчислювальної техніки призвели до того, що на сучасному етапі захист комп'ютерних систем від несанкціонованого доступу характеризується зростанням ролі програмних та криптографічних механізмів захисту в порівнянні з апаратними.

Зростання ролі програмних і криптографічних засобів захисту проявляється в тому, що виникають нові проблеми в галузі захисту обчислювальних систем від несанкціонованого доступу, вимагають використання механізмів і протоколів з порівняно високою обчислювальною складністю і можуть бути ефективно вирішені шляхом використання ресурсів ЕОМ.

Виникнення глобальних інформаційних мереж типу INTERNET є важливим досягненням комп'ютерних технологій, однак, з INTERNET пов'язана маса комп'ютерних злочинів.

Результатом досвіду застосування мережі INTERNET є слабкість традиційних механізмів захисту інформації та відставання у застосуванні сучасних методів.

Криптографія надає можливість забезпечити безпеку інформації в INTERNET і зараз активно ведуться роботи з впровадження необхідних криптографічних механізмів в цю мережу. Не відмова від прогресу в інформатизації, а використання сучасних досягнень криптографії - ось стратегічно правильне рішення. Інформація повинна бути захищена в першу чергу там, де вона створюється, збирається, переробляється і тими організаціями, які несуть шкоди безпосередній при несанкціонованому доступі до даних. Цей принцип є як раціональний так і ефективний: захист інтересів окремих організацій – це складова реалізації захисту інтересів держави в цілому.

Список використаних джерел

1. *Означення поняття криптографя[Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Криптографія.*
2. *Про проблеи захисту інформації в комп`ютерних мережах [Електронний ресурс]. – Режим доступу: http://ua-referat.com/.*
3. *Про завдання захисту електронної інформації [Електронний ресурс]. – Режим доступу: http://ua.textreferat.com/.*

Розділ І

Захист об'єктів інформації, інформаційних систем підприємств, установ та організацій від протиправних посягань

1.1. Інформаційна система підприємства

Ефективне функціонування підприємства (організації) неможливе без управління ресурсами, що використовуються для досягнення мети. Згідно з поширеними нині в управлінській літературі поглядами поняття ресурси охоплює не лише людей, капітал, сировину, а й інформацію.

Зміст цілеспрямованої діяльності підприємства зводиться до виявлення необхідних ресурсів і перетворення їх у корисну продукцію.

Нині не лише з теорії, а й з багаторічної практики відомо, що як природні ресурси, так і інформація для суспільства завжди обмежені. Попит на інформацію набагато перевищує можливості його задовольнити. Річ у тому, що в процесі діяльності підприємства потенційна інформація циклічно актуалізується, тобто виникає потреба в її використанні саме в той момент, коли необхідно приймати управлінське рішення, наприклад, з приводу укладання договору.

Для задоволення інформаційних потреб підприємства необхідно створити оптимальну структуру з визначенням вимог, що висуваються для забезпечення інформаційної безпеки.

Принципово важливо, щоб інформаційна структура відповідала розподілу повноважень на підприємстві, а необхідна для вирішення завдань інформація надавалася у підрозділах не будь-кому, а лише відповідальним особам. Інформаційна структура має бути побудована таким чином, щоб задовольняти потреби усіх рівнів управління підприємством. Саме такий підхід дасть змогу правильно й оптимально вирішити проблему створення корпоративної мережі підприємства (установи).

Корпоративна мережа підприємства (установи) — це організація зв'язку в інформаційній системі корпорації через відомчу глобальну мережу, тобто обмін інформацією між кількома розміщеними на достатньо великій відстані один від одного ПК, об'єднаних локальною мережею.

Необхідно пам'ятати, що інформація суттєво відрізняється від інших видів ресурсів підприємства, а саме — її дані характеризують процеси, що протікають як у самому підприємстві, так і поза ним.

Зміст управління видами діяльності підприємства залежить насамперед від змісту і способів отримання ним інформації. Інформація, що стосується сировинних матеріалів, грошових засобів, технологічних процесів, у науковій літературі відноситься до забезпечувального фактора управління виробництвом.

Щодо іншої сторони інформації, то вона сама є особливим видом ресурсів, а тому для досягнення поставленої мети необхідно здійснювати вплив за допомогою відповідної сукупності прийомів на процеси накопичення, зберігання, поширення і використання даних на рівні підприємства. В цьому випадку інформація виступає об'єктом управління.

Багатоплановий підхід до інформаційних ресурсів обумовлює необхідність враховувати такий суттєвий фактор, як функціонування підприємства за умов ринкових відносин, характерною прикметою яких є боротьба між незалежними суб'єктами господарювання на ринку і гостра конкуренція товаровиробників. Боротьба за економічне виживання — закон ринку [29].

Забезпечення безпеки підприємства за умов ринкових відносин потребує захисту підприємницької інформації, яка в спеціальній літературі розглядається як умова, що допомагає або створює перешкоди у досягненні позитивного результату (прибутку) в господарській діяльності [45, *55–56*].

Підприємницька інформація, що створює суб'єктові вигідні умови для прийняття оперативних рішень і досягнення ефективного результату, вважається корисною. Для її захисту від сторонніх осіб, щоб не втратити очікування, як правило, застосовується комплекс методів технічного й організаційного характеру.

Підприємницька інформація, що циркулює в ринково-конкурентній сфері діяльності, поділяється на організаційну, техніч-

ну, комерційну, фінансову, рекламну, є також інформація про попит і пропозицію, конкурентів, чинне законодавство, кримінальне становище, включаючи відомості про способи, сили і засоби забезпечення безпеки інформації в корпоративній мережі підприємства тощо [75].

Інформація про діяльність підприємства зберігається в різних формах: у пам'яті людини, картотеках, книгах обліку, на накопичувальних пристроях ЕОМ та ін.

Необхідно звернути увагу на деякі питання, пов'язані з практичним використанням технічних засобів для зберігання, видачі, обробки і пошуку інформації [60].

Інформаційна структура має відповідати організаційній структурі управління підприємством, але необов'язково її ототожнювати. Розв'язання завдань управління направлене на об'єднання всіх видів ресурсів і потоків інформації в єдиний процес досягнення мети.

Вагоме місце в технології управління посідає інформаційне поле — носії потенційної інформації, що необхідна для успішного виконання підприємством своїх завдань і функцій.

Існують взаємопов'язані технології функціонування (виробничі технології), але вони різняться за своїми характеристиками.

Управлінська технологія забезпечує процес управління підприємством (установою).

Для глибшого осмислення управлінської технології важливо виділити її елементи. До них належать: інформація, операція і методи здійснення управлінських технологій, персонал, обладнання, структура [55].

Необхідно пам'ятати, що підрозділи в складі інфраструктури підприємства пов'язані через свої властивості та завдання, що вирішуються. В цілому наявність тієї чи іншої структури з притаманними їй елементами у складі підприємства зумовлена необхідністю їх об'єднання в технологічний процес. На наш погляд, з'ясування цих обставин важливе з погляду роз'яснення значення безпеки інформації в корпоративній мережі, оскільки велика кількість підприємств має доступ до мережі Інтернет. Безперечно, це добре, з одного боку, а з іншого — усі країни світу мають доступ до внутрішньої корпоративної мережі.

Найсучаснішим обладнанням в управлінській технології є ПК (персональні комп'ютери), а також стаціонарні і рухомі засоби зв'язку. Серед них можна виділити:

- технічні засоби для обробки інформації та захисту каналів її циркулювання (фіксування, передачі, пошуку, обробки інформації);
- носії інформації — матеріальні предмети, за допомогою яких і передається інформація.

Наближеним до поняття інформаційне поле є поняття комунікаційний простір підприємства, тобто та частина середовища його функціонування, в якій він має змогу, за допомогою наявних сил і засобів, управляти інформаційними процесами, зокрема процесом актуалізації потенційної інформації. Однак комунікаційний простір підприємства може бути суттєво збільшено шляхом об'єднання з іншими інформаційними системами (наприклад, Інтернет).

Слід зазначити, що на сьогодні управлінські інформаційні технології не мають реальної альтернативи магнітному зберіганню інформації.

В інформаційних системах, базовим елементом яких є комп'ютер, основна інформація зберігається на жорстких магнітних дисках. Саме у накопичувачу на жорстких магнітних дисках (НЖМД) зберігається і з нього завантажується в оперативну пам'ять комп'ютера операційна система, інформація обробляється в процесі використання, а використана знищується.

Один з найважливіших показників — енергетична незалежність робить НЖМД практично незамінним для оперативного і довготривалого зберігання великих масивів інформації. Накопичувач на жорстких магнітних дисках, як правило, називають вінчестером.

Необхідно зазначити, що в наш час великі обсяги інформації зберігаються, обробляються та передаються електронними засобами і, відповідно, супроводжуються електромагнітним випромінюванням. Тому існує реальна можливість несанкціонованого доступу до цієї інформації за допомогою радіоперехоплення або контактного підключення до комунікацій [39, *104–108*].

Комп'ютер у режимі автономної роботи нині практично не застосовується. На автономних комп'ютерах здійснюється обробка і зберігання інформації, а за окремого підключення або за

підключення до глобальної мережі Інтернет — і передача інформації (обмін інформацією).

У локальній мережі здійснюється весь обсяг роботи з інформацією: зберігання, обробка і передача.

Персональний комп'ютер є центральною ланкою в системі автоматизованої обробки інформації і привертає особливу увагу конкурентів, правопорушників і розвідувальних служб [54, *20–24*]. Для отримання цінної інформації вони застосовують усі доступні засоби і методи, серед них і різноманітні типи аналізаторів, що підключаються до ліній електроживлення.

Тому найжорсткіші вимоги до захисту інформації мають встановлюватися для комп'ютерів локальної обчислювальної мережі, усі елементи якої пов'язані між собою кабельною системою (як правило, екранована або неекранована плетена пара). Локальну комп'ютерну мережу нині недоцільно використовувати автономно, без взаємодії з іншими мережами.

1.2. Загальнотеоретичні характеристики окремих напрямів захисту від перехоплення інформації, що обертається у локальних та корпоративних мережах установ і підприємств

Розвиток комп'ютерних технологій і їх використання в багатьох сферах економіки є на сьогодні одним з головних факторів її ефективності. Проте прогрес в інформаційно-технічній сфері створив і потенційні загрози у вигляді розроблення нових та удосконалення вже відомих методів наукового шпигунства, котрі дозволяють швидко знаходити в комп'ютері необхідні відомості.

Збирання інформації про розробки високих технологій завжди було і залишається одним з пріоритетів у діяльності розвідок світу [87]. Тому дедалі активніше застосовуються перевірені на практиці методи отримання відомостей від учасників науково-практичних конференцій, організаторів виставок, обслуговуючого персоналу.

Перехоплення секретної інформації, що обробляється з використанням засобів обчислювальної техніки і передається лінія-

ми зв'язку абонентів, здійснюється за допомогою портативних розвідувальних радіоприймачів, забезпечуючи багатоканальний прийом сигналів з різних напрямків і на різних частотах. Такий спосіб радіорозвідки набув найбільшого поширення [89, *70*]. Хоча необхідно зазначити, що арсенал спеціальних технічних засобів і методів, що використовуються для викрадення секретних відомостей з інформаційних систем підприємств, установ, корпорацій, досить широкий.

Здобуття конкуруючими комерційними фірмами цінної інформації може здійснюватися шляхом введення в комп'ютерну систему (зокрема в графічні і звукові файли) спеціальної програми-закладки для таємного передавання даних, що містяться у знайдених нею файлах. Програма дозволяє не лише надійно приховати факт передавання повідомлення, а й зашифрувати його за допомогою криптоалгоритму. Поряд з методами перехоплення певний інтерес викликають засоби таємного стеження за екраном монітора за допомогою випромінюваних електромагнітних хвиль, що виникають під час оброблення інформації в комп'ютері [28].

Якщо відеомонітор, як правило, недосяжний для огляду випадковим особам, оскільки його встановлюють таким чином, щоб не можна було розглянути екран, то в оптичному діапазоні отримати інформацію все таки можливо, але з світлового випромінення монітора.

Зображення на екрані відеомонітора після численних відбивань від різних поверхонь (стін, стелі, меблів та інших предметів) можна перехопити спеціальною технікою, що дозволяє перетворити світловий потік в іншу відеоінформацію. Перехоплення композитного сигналу з екрана відеомонітора не викликає будь-яких перешкод, скажімо, у вигляді мерехтіння на поверхні дисплея. Проте така оптико-електронна розвідка потребує чимало часу, інколи тижні. Спеціалісти науково-дослідних установ, які займаються проектуванням і створенням нової техніки, мріють "примусити" комп'ютер передавати інформацію тоді, коли це необхідно для таємного спостереження [40]. Зміст ідеї вчених зводиться до зараження потрібного комп'ютера спеціальною програмою-закладкою ("троянський кінь") будь-яким з відомих способів за технологією вірусів, зокрема, через дискету з драйверами, а якщо персональний комп'ютер під-

ключений до системи локальної обчислювальної мережі, то через неї.

В інформаційних мережах, базовим елементом яких є комп'ютер, основні обсяги інформації зберігаються на жорстких магнітних дисках. Саме тому програма-закладка шукає необхідну інформацію на них і, звертаючись до різних електричних пристроїв, викликає паразитні випромінення електромагнітних коливань у просторі. За допомогою такої програми можна вмонтувати в композитний сигнал відеомонітора повідомлення, що містить розвідану інформацію. При цьому користувач ПК, наприклад, граючи на комп'ютері в карти, візуально не може визначити, що вони містять у собі ще й певну інформацію у вигляді секретних текстових повідомлень [81].

Для забезпечення перехоплення паразитного випромінення монітора і виділення необхідного корисного сигналу необхідно мати розвідувальний приймач (у найпростішому вигляді — звичайний доопрацьований телевізор). Експериментальні дослідження, проведені в різних країнах, підтверджують можливість отримання таємної інформації шляхом приймання паразитного випромінення композитного сигналу відеомонітора. Результатом усіх цих досліджень стала технологія SOPFT TEMPEST — технологія таємного передавання даних каналами паразитних електромагнітних випромінень за допомогою програмних засобів.

Звернемо увагу на основні передумови історії виникнення TEMPEST як технології розвідувальної діяльності, націленої на перехоплення інформації, опрацьованої в локальних обчислювальних мережах, і захисту інформації від відтоку через канали паразитних випромінень і наведень. Необхідно звернути увагу, що серед спеціалістів утвердився подвійний підхід до цієї технології і вони вважають TEMPEST, з одного боку, як засіб нападу (розвідки), а з іншого, як засіб захисту.

У 1918 р. Герберт Ярдли зробив принциповий висновок, що різні електронні пристрої для оброблення секретної інформації мають паразитні випромінення, їх можна використовувати для відновлення, перехоплення зашифрованих повідомлень. З метою забезпечення комунікаційної безпеки (COMSEC) у 1946 р. була заснована Канадська Організація захисту зв'язку (CSE).

У нашій країні також проводиться робота щодо захисту інформації від відтоку каналами побічного випромінення —

ПЕМВН (побічні електромагнітні випромінення і наведення). В Європі та Канаді застосовується термін Telecommunications Electronics Material Protected Form — компрометуюче випромінення, а в Америці — "TEMPEST", під цією абревіатурою прихована назва таємної програми Міністерства оборони Америки з розробки методів попередження відтоку інформації через демаскуюче і побічне випромінення електронного обладнання.

Дбаючи про концентрацію зусиль щодо захисту інформації, згідно з указом Президента України на базі Головного управління урядового зв'язку СБ України в 1999 р. було створено Департамент спеціальних телекомунікаційних систем і захисту інформації СБ України. Це та головна структура в державі, що займається питаннями криптографічного і технічного захисту інформації.

Застосування в управлінській технології електронного документообігу в цілому створює можливість несанкціонованого доступу до комунікацій. Відтік інформації з обмеженим доступом, що має реальну цінність, напряму пов'язаний з очікуваними результатами. І саме це може завдати значної шкоди інтересам власника інформації [14].

Тепер розглянемо питання несанкціонованого зняття інформації, що зберігається на НЖМД. Кому не відомо, що в процесі експлуатації комп'ютера інколи з ладу виходять різні електронні пристрої, серед них може бути і накопичувач на жорстких магнітних дисках.

У відповідності з чинними законодавчими актами, що регулюють відносини між споживачами товарів і виробниками, продавцями і виконавцями за умов різноманітних форм власності, виробник забезпечує нормальну роботу товару, зокрема і комплектуючих деталей, протягом гарантійного строку, встановленого законодавством, а у випадку його відсутності — договором. Гарантійними зобов'язаннями, що зазначені у договорі, передбачена заміна НЖМД, але лише за умови збереження пломб і дотримання правил експлуатації комп'ютера.

Деякі користувачі ПК, відправляючи несправний НЖМД до сервісного центру, часто інформацію на ньому не знищують. Так постачальнику комп'ютерної техніки добровільно передається інформація, зокрема й конфіденційна.

Слід зазначити, що вітчизняні постачальники комп'ютерної техніки закуповують комплектуючі вироби у зарубіжних виробників через їх представників. Щоб обміняти несправний накопичувач на НЖМД належної якості, його відправляють зарубіжному представникові.

Нестандартну поведінку користувача ПК можна зрозуміти. Техніка "відмовляє", образно кажучи, в найкритичніший час, та й з усталеної практики експлуатації накопичувача з гарантійним і післягарантійним обслуговуванням виникає ситуація, що має суперечливий характер.

Порушення звичної діяльності користувача ПК у поєднанні з опосердкованим тиском керівництва, яке вимагає негайно усунути недолік, справляють сильний вплив на поведінку людини, що досить часто стає на перешкоді до належного виконання нею службових обов'язків, заважає критично оцінити ситуацію, що склалася. А буває й таке. Виникає потреба знищити зайву інформацію. В такому разі вдаються до стандартної операції. Засоби візуалізації комп'ютера інформують користувача про знищення файлу. Насправді ж інформація як і раніше зберігається на НЖМД і може бути поновлена. А зникли лише посилання на неї в каталозі та в таблиці розміщення файлів. Отже, проблема полягає у належному знищені інформаційних відходів [39].

Цікаво, до речі, розглянути технологію розподілу інформації у базі даних ЕОМ. Виявляється, що відомості, які зберігаються там, зафіксовані на жорстких або гнучких дисках і можуть бути роздруковані (лістинг). Як відомо, в основу функціонування вінчестера покладено принцип магнітного запису, тобто зчитування сигналів на обертаючому диску, що покритий магніточутливим робочим шаром. При зчитуванні ділянки диска з різною намагніченістю рухаються під магнітною головкою й індукують у ній електромагнітні сигнали, що перетворюються на цифрові дані.

Сучасний накопичувач на жорстких дисках складається з: блока (пакета), дисків, шпиндельного двигуна — приводу обертання дисків, блока головок запису/зчитування, посилювача — комутатора головок і контролера — друкованої плати з електронними схемами управління.

Гарантоване знищення інформації при виведенні накопичувача з експлуатації, на думку спеціалістів, зокрема компанії

“ЕПОС”, котра є ліцензіатом Департаменту спеціальних телекомунікаційних систем і захисту інформації СБ України, досягається шляхом запису на місце знищеного файлу іншої інформації і наступним її знищенням засобами операційної системи. Для цього існують спеціальні програми, зокрема, одна з них є у комплексі Нортоновських утиліт. Нова інформація записується на стару, знищуючи її. Багаторазовий запис на місце інформації, що знищується, випадкових (шумоподібних) наступностей пошкоджує магнітну структуру лише тих ділянок доріжок, на яких зберігалися дані, що підлягають знищенню. Перезапис — це процес запису нетаємних даних у пам’ять, де раніше зберігалися таємні дані. Під час перезапису інформаційна працездатність накопичувача на жорсткому магнітному диску зберігається, якщо він був цілком несправним. На зношеному НЖМД надійно знищити інформацію неможливо.

Методи знищення інформації поділяються на безпрограмні, механічні, фізичні, а за засобами впливу на пристрій НЖДМ:

- без знищення конструктивної структури і поверхні НЖМД;
- зі знищенням НЖМД.

Механічні методи знищення інформації на НЖМД за способом впливу на носій поділяються на механічні, термічні, піротехнічні, металотермічні, хімічні, радіаційні.

Знищити інформацію можна шляхом впливу на диски міцним постійним або тимчасовим магнітним полем (знищується магнітна структура робочих поверхонь).

Гарантоване знищення інформації з магнітного носія турбує багатьох користувачів, тому певний інтерес викликає поширений нині в спеціальній літературі погляд на це. Гарантоване знищення інформації з магнітного носія — це такі зміни його магнітної структури, за яких неможливе зчитування інформації стандартними засобами накопичувача, а поновлення втрачених даних, що зберігаються на жорстких дисках, за допомогою спеціальних методів економічно недоцільне.

1.3. Захист інформації від відтоку через канали побічного електромагнітного випромінення і наведень комп'ютера

У зв'язку з бурхливим розвитком локальних і глобальних обчислювальних мереж удосконалюються і методи розвідки (комерційного шпигунства), спрямовані на перехоплення інформації, що обробляється, передається, зберігається у локальних мережах [45]. Нині важко відповісти — розвідувальною діяльністю більше займаються на рівні держав чи комерційних фірм, підприємств-конкурентів [12]. Відповідно, швидко удосконалюються і методи протидії розвідці [84]. Необхідно зазначити, що ввійти у локальну мережу будь-якої організації можна *лише при некваліфікованому налагодженні* всіх елементів локальної мережі (кожного окремого комп'ютера) адміністратором системи. Якщо правильно застосовуються наявні заходи щодо захисту від несанкціонованого входження в локальну мережу ПК, а також додаткові програмні й апаратні засоби, своєчасно виконуються необхідні організаційні заходи, шпигун вимушений відшукувати нові прийоми і засоби, щоб здобути інформацію.

Не випадково останнім часом бурхливо розвиваються методи *перехоплення* інформації за допомогою каналів побічного електромагнітного випромінення і наведень (ПЕМВН) елементів локальної мережі ПК [80].

Забезпечення інформативної безпеки в корпоративних, міжкорпоративних, локальних обчислювальних та інших автоматизованих системах нині набуло особливої актуальності [19]. До захисту периметру корпоративної мережі інженерно-технічний персонал ставиться досить серйозно [11]. За даними статистики, основним джерелом загрози безпеці корпоративної мережі, як і раніше, залишаються саме легальні користувачі. Тому слід посилити увагу до організації технічного захисту інформації в корпоративній мережі, а саме:

- збереженню цілісності будь-якої оперативної інформації підприємства, насамперед конфіденційної;
- забезпеченню безперервної роботи обладнання.

Розголошення або втрата інформації може не лише спричинити фінансові збитки, а й завдати шкоди репутації і конкурентоздатності фірми. Не менш важливим є і безперервна робота об-

ладнання — вихід із ладу того чи іншого вузла призводить як до витрат на його відновлення, так і до припинення обслуговування клієнтів, що означає зниження прибутків.

Відтік або втрата конфіденційної інформації та вихід з ладу обладнання може статися внаслідок:

- незумисних помилок користувача;
- умисних шкідливих дій користувача;
- таємного введення в систему програм-закладок з вірусами "троянський кінь", "червяк" тощо [48].

Значна кількість важливої інформації зберігається не лише на *файл-сервері,* а й на робочих станціях (комп'ютерах) користувача. Ці дані можуть бути легко втрачені або розголошені, якщо не вживати відповідних заходів. Насамперед рекомендується використовувати файлову систему NTFS для системного поділу жорсткого диска, що забезпечує ряд додаткових можливостей для захисту від перехоплення секретної інформації через канали ПЕМВН.

Одна з таких можливостей — управління доступом. За допомогою списку управління доступом (ACL) можна обмежити доступ до комп'ютера як для окремого, так і для групи користувачів. Наприклад, один з користувачів зможе читати зміст файлу, інший — вносити до нього зміни, а всі інші взагалі позбавлені доступу до файлу. Це необхідно, коли на одному комп'ютері працює кілька користувачів або в мережі підприємства не встановлено обмежень на їх реєстрацію і будь-який користувач, який має фізичний доступ до комп'ютера, може зареєструватися на ньому. В операційній системі Windows 2000 використовується п'ята версія NTFS — файлова система. Однією з її новинок є шифрована файлова система [Encrypting File System, EFS], що дає можливість обмежувати доступ до файлів і папок.

Локальна комп'ютерна мережа нині не може експлуатуватися автономно, без взаємодії з іншими мережами. Будь-яка організація, чи то приватне підприємство, чи орган державного управління, прагне бути представленим в глобальній мережі Internet — власним сайтом, загальнодоступною електронною поштою, доступом співробітників до інформації в глобальній мережі. Саме це і потребує суворо дотримуватися вимог інформаційної безпеки. Річ у тому, що взаємовплив деяких мереж може викликати різні загрози для установи.

Найбезпечнішою з усіх можливих загроз при підключені до глобальної мережі Internet є злам мережі з хуліганських мотивів. Найтиповішим проявом вандалізму в Internet є заміна діючих посилань на посилання порнографічних сайтів. Це шкодить іміджу власника сайта і призводить до додаткових витрат на відновлення усіх посилань.

В комп'ютерних мережах державних органів влади, підприємств України є цікава інформація для іноземних фірм, що беруть активну участь у комп'ютерній боротьбі. Вона може й не мати грифу таємності, однак у сукупності дає змогу отримати дуже важливі відомості. Тому в разі об'єднання комп'ютерних мереж державних установ, підприємств, науково-дослідних інститутів та організацій з глобальною мережею — Інтернет слід очікувати, окрім хуліганських зламів мережі, і кваліфікованого проникнення до корпоративної мережі установи [41]. (*Корпоративний — такий, що належить до будь-якої корпорації*). Протидіяти цьому дуже складно. Тому мережу Інтернет необхідно ізолювати від внутрішньої, де зосереджені узагальнені дані. Для ізоляції власної комп'ютерної мережі від глобальної використовується ряд способів з метою захисту від перехоплення спеціальними розвідувальними приймачами випромінених комп'ютерами електромагнітних коливань.

В мережах, в яких не обертається інформація з обмеженим доступом, для ізоляції, як правило, досить використати фільтруючий **маршрутизатор**, що виконує роль **брандмауера**, тобто шлюзу, який закриває інформаційні ресурси внутрішньої мережі підприємства. Захист від проникнення з глобальної мережі можна забезпечити лише за допомогою міжмережевих екранів. Найповніша безпека гарантується лише за *фізичної ізоляції мережі Інтернет* від власної локальної. За необхідності протидіяти іноземним розвідкам це виправданий захід. Постановою Кабінету Міністрів України від 12 квітня 2002 р. в Україні заборонено підключати до глобальних мереж обчислювальні мережі й окремі комп'ютери, на яких обробляється та зберігається інформація з обмеженим доступом, власником якої є держава [6].

При побудові фізично розділених мереж необхідно приділяти увагу захисту відтоку інформації через канали ПЕМВН. Досить часто співробітнику, який працює з інформацією з обмеженим

доступом, необхідно увійти в Інтернет. Для забезпечення такої можливості на робочому місці встановлюється два комп'ютера, один з них підключається до локальної мережі підприємства, а другий — до мережі Інтернет. У даному випадку виникають ускладнення від того, що кабелі власної мережі з захистом інформації та кабелі відкритої мережі Інтернет важко розмістити на достатній відстані. Тому інформація, що обертається в локальній мережі, а також усі паразитні випромінення комп'ютерів, наведені на кабелі локальної мережі, можуть наводитись і на кабелі відкритої мережі Інтернет. Для відкритої мережі характерно, що її прокладають, як правило, неекранованими кабелями і вона являє собою досить довгу антену, що виходить за межі кордонів захищеної території. Саме тому отримати інформацію можна не лише шляхом перехоплення випромінення, а й безпосередньо через підключення до кабелів відкритої мережі [61].

Можливість отримати інформацію за автоматизованої її обробки шляхом перехоплення паразитного радіовипромінення багатьма не сприймалася серйозно. Цілком можливо, що це зумовлено психологією людини (багатоманітність поглядів, часто помилкових). Люди, як правило, неохоче вірять у те, чого вони не бачили своїми очима. Проте досвід багатьох країн доводить, що успішні спроби отримання інформації за рахунок перехоплення побічних електромагнітних випромінень ніколи не розголошуються. Вагоме значення для розуміння методики захисту інформації від відтоку через канали паразитного випромінення і прослуховування розмови поруч з комп'ютером має широко відомий у радіотехніці "мікрофонний ефект". Він створюється корпусом електронного пристрою під впливом акустичних коливань.

Для розв'язання завдань зі сфери технічного захисту інформації на практиці найчастіше застосовують два основні методи: *активний і пасивний* [58].

Активний метод передбачає застосування спеціальних широкосмугових передавачів перешкод. Активними є ті перешкоди, що виникають від сторонніх джерел електромагнітних коливань. Для створення загороджувальної активної перешкоди застосовується шумова перешкода. Залежно від принципу генерування розрізняють шумові і прямошумові перешкоди. Прямошумова перешкода являє собою безпосередньо шумову напругу

в порівняно широкому діапазоні високих частот. У такої напруги відсутня явно виражена несуча частота і міць передавача перешкод розподіляється рівномірніше по всьому спектрові шумової перешкоди, тому такий вид перешкоди є досить ефективним. Спектр шумової перешкоди може бути значно більшим від смуги пропуску приймального тракту малогабаритного професійного розвідувального приймача.

Активний метод радіопротидії досить результативний, оскільки за його допомогою усувається не лише загроза відтоку інформації через канали паразитного випромінення комп'ютера, а й унеможливлюється застосування закладних прослуховуючих пристроїв, перехоплення електромагнітних коливань, що випромінюються іншими радіотехнічними засобами, розміщеними в захищеному приміщені [58].

При оцінці ефективності цього методу необхідно брати до уваги як об'єктивну, так і суб'єктивну сторони процесу. Це зумовлюється тим, що два різні суб'єкти, один з яких займається технічною розвідкою, а інший технічним захистом інформації, з огляду на свої завдання неоднаково сприймають кінцевий результат.

Відомо, що, застосовуючи будь-який метод технічного захисту інформації, спеціаліст обов'язково зіткнеться як з його недоліками, так і з перевагами. Активному методу захисту властиві такі недоліки. По-перше, застосовується досить потужне джерело випромінення, що вважається шкідливим для здоров'я. По-друге, наявність маскуючого випромінення в ефірі свідчить про те, що в приміщені встановлені засоби радіопротидії, які ускладнюють застосування радіорозвідувальних систем виявлення витоку інформації через канали паразитного випромінення.

Щодо об'єктивності оцінки активного методу захисту інформації, то вона перебуває у прямій залежності як від можливості перехоплення за допомогою розвідувального приймача електромагнітних коливань, так і від прослуховування розмов біля комп'ютера за допомогою малогабаритного професійного розвідувального приймача.

Аналіз практики свідчить, що успішне застосування методів і засобів захисту від загроз відтоку інформації багато в чому залежить від правильного вибору, в кожному конкретному випадку, адекватних приборів, пристроїв, апаратури, а також від-

повідності технічних засобів вимогам допустимості. Застосування технічних засобів, як відомо, можливе, якщо гарантується дотримання правомірності, безпеки, нешкідливості, морально-етичних норм суспільства.

Некритичне сприйняття недоліків і переваг того чи іншого методу захисту інформації може призвести до серйозних втрат у розробці технічних рішень забезпечення безпеки інформації в корпоративній мережі установи. Особливо важливо відзначити, що невдала, на перший погляд, спроба перехоплення випромінених комп'ютером електромагнітних коливань за допомогою радіоелектронних засобів розвідки і водночас виявлення спеціального генератора перешкод дозволяє дійти висновку про наявність у даній установі секретів, що приховуються на професійному рівні.

Залежно від індивідуальних особливостей побудови структури мережі установи, в якій обертається інформація, поряд з активним методом її захисту від відтоку через канали паразитного випромінення комп'ютера і наступного перехоплення може застосовуватися пасивний метод.

За *пасивного методу* захисту інформації від перехоплення джерело випромінення, як правило, екранується — комп'ютер встановлюється в екранованій шафі. Екранування можна досягти і в такий спосіб: на двері, стіни, підлогу, стелю покласти металеві листи.

Для банківських установ України вимоги до екранування приміщень, в яких встановлена обчислювальна техніка, закріплені відомчими нормами ВБН В.2.2–00032106–1–95. Зокрема, передбачено обов'язкове екранування тих кімнат і боксів, в яких розміщено сервери корпоративної мережі та Інтернет. Відповідною нормою регулюється порядок проведення робіт з перевірки ефективності екранування по всьому периметру захищеної від випромінення зони. Питання щодо виявлення ефективності екранування можуть бути вирішені за допомогою такого методу, як вимірювання рівня сигналів, випромінюваних комп'ютером. Поняття ефективності як технічної категорії має передусім практичне значення.

Оцінка ефективності застосовуваних методів захисту інформації (активного або пасивного) потребує інструментального підтвердження реальних наслідків їх реалізації, тобто, чи уне-

можливилася розвідка з використанням каналів побічного електромагнітного випромінення комп'ютера та інших радіоелектронних засобів, що розміщені в екранованому приміщені.

1.4. Превентивні дії на захист інформаційних ресурсів підприємства від посягань зловмисників

Останнє десятиріччя позначилося бурхливим розвитком підприємницької діяльності в Україні. Багато підприємств почали активніше вдаватися до нових управлінських технологій. Для реалізації методів управління широко застосовують персональні комп'ютери, впроваджують сучасні системи зв'язку. Пошук, обробка, передача інформації здійснюються, як правило, через персональний комп'ютер.

Управлінська технологія, поряд з переробкою специфічного ресурсу організації — інформації, забезпечує процес управління підприємством. Результатом різних видів діяльності в управлінні є варіанти управлінських рішень, обмін якими відбувається шляхом передачі визначеної інформації. Тому за правильної організації взаємодії в системі, тобто у підприємстві та в зовнішньому середовищі, може бути досягнуто перетворення управлінських відносин у цілеспрямовані зв'язки.

Ми погоджуємося з думкою, викладеною в літературі, згідно з якою в усіх видах управлінської діяльності передбачається наявність комунікативних пов'язаних процесів.

Зміст ролі людини в інформаційному процесі управлінської технології — це не стільки прийом, передавання та поширення інформації, скільки складний процес впливу на людей для досягнення мети [31].

Можна погодитися з А. Г. Додоновим, Є. С. Горбачиком, М. Г. Кузнецовою у тому, що "в інформаційному суспільстві багато функцій у прийнятті рішень підтримуються технічними системами, проблема уразливості цих систем до неумисних помилок персоналу і умисному спеціальному впливу з зовні стає проблемою безпеки суспільства і держави"*.

---

* А. Г. Додонов, Е. С. Горбачик, М. Г. Кузнецова. Проблемы безопасности в информационном обществе // Информационная безопасность офиса: Научно-практ. сборник. — Вып. 1 "Технические средства защиты информации". — К.: ООО "ТИД "ДС", 2003. — 216 с.

Необхідність у захисті інформації значною мірою пов'язана з переходом економіки України до ринкових відносин. У переважній більшості робіт, присвячених проблемам інформаційної безпеки підприємництва в Україні, зазначається, що для забезпечення ефективного застосування заходів захисту потрібні специфічні знання [61, *65–76*].

В останні роки помітний значний розрив між можливостями застосування різних наук (кібернетики, теорії інформації, радіотехніки, електротехніки, криміналістики тощо) для захисту підприємницької інформації і станом розробки методів та засобів протидії посяганням на господарюючих суб'єктів.

Проблема захисту підприємницької інформації на сьогодні розроблена недостатньо. В літературі не знайти чіткого визначення інформаційної безпеки підприємства. Залишаються не досить глибоко дослідженими такі важливі поняття, як захищеність інформації, захисні засоби, що застосовуються для досягнення поставленої мети, і система комплексних захисних заходів [56]. Не розроблена концепція комплексного захисту підприємницької інформації [20].

Організація захисту підприємницької інформації потребує розробки науково-методичних основ, практичних рекомендацій, прийомів і способів, що забезпечують безпеку в діяльності господарюючого суб'єкта .

Успішне розв'язання поставленого завдання передбачає насамперед об'єднання результатів досліджень у галузі комп'ютерної інформації і тієї, що є об'єктом інтелектуальної власності (ноу-хау, конфіденційна інформація, банківська, комерційна таємниця), в рамках основ захисту підприємницької інформації [76].

Проблема захисту підприємницької інформації в науковій літературі висвітлена переважно у плані загальнотеоретичної характеристики окремих її аспектів [88]. Вагомий внесок в осмислення проблеми захисту підприємницької інформації зробили: М. Алещенков, Б. Радіонов, А. Хорєв, А. Задворний, Д. Халяжин, В. Ярочкін, В. Ліпкан, П. Біленчук, М. Гуцалюк, В. Герасименко, В. Попович, Л. Хофман, А. Доджонов, В. Цимбалюк.

У роботі, поряд з викладенням досвіду авторів, використовуються матеріали літературних джерел, присвячених захисту інформації, яка опрацьовувалася засобами обчислювальної техніки і оберталась у мережах, що побудовані на їх базі [70].

Автори, обґрунтовуючи теоретичні позиції комплексного вирішення проблеми захисту підприємницької інформації, безпосередньо спиралися на праці, у яких досліджуються питання інформаційної безпеки, спеціальної техніки, захисту комерційної таємниці і конфіденційної інформації, кримінології, насамперед С. Коженевського, С. Чеховського, В. Освяннікова, Г. Солдатенко, Ю. Рудакова, Є. Ф. Толмачова, А. Долгової, В. Ліпка, Г. Нікіфорова, С. Нікіфорова, А. Провозіна, Г. Векслера, І. Зємана, А. Чернявського, Н. Чистякова, В. Смольнікова, Б. Вікторова, Я. Бельсона, В. Шамрая.

Необхідною умовою успішного функціонування підприємства, що розглядається як суб'єкт управління в підприємницькій діяльності, є всеохоплюючий інформаційний обмін всередині організації і з її зовнішнім середовищем [68].

Якщо давати оцінку змісту поняття "інформація" з психологічного погляду, то воно стоїть в одному ряду з близьким до нього за значенням "дані". Дані перетворюються в інформацію, якщо людина оцінила їх значення і користь. Дані можуть розглядатись як ознака або записані спостереження, що в даний момент не впливають на поведінку суб'єкта або об'єкта.

Відомо, що інформація зберігається в різному вигляді і передається різними каналами. До основних носіїв інформації належать: ознайомлені особи, документи, засоби зв'язку і комунікації, апаратура передавання даних, електронні системи опрацювання, зберігання і розподілу інформації.

Інформація в системі управління — це дані, що характеризують процеси, які протікають в організації та у зовнішньому середовищі. Інформація, що виникає і використовується всередині мережі суб'єкта господарювання має назву "внутрішня".

Інформація є найважливішим ресурсом в управлінні. В ній знаходять відображення характеристики усіх інших видів ресурсів, а також події, що відбуваються в організації та у зовнішньому середовищі. Ресурси являють собою засоби досягнення мети організації.

До інформації, що потребує захисту, П. М. Клименко відносить "інформацію, котра визнається діловою, виробничою, торгівельною, якщо вона є економічно цінною, корисною в підприємницькій діяльності, невідомою широкому загалу, недоступною для комерційних кіл і конкурентів. Обов'язковим елементом

ції інформації (в т. ч. технічної чи ділової) є і корисність, що забезпечує довготермінові переваги власника перед конкурентами у виробничій, комерційній, дослідницькій або іншій діяльності, а також може забезпечити підвищення ефективності управління" [58, *283–289*].

За всього розмаїття визначень захищеності інформації більшість учених, які працюють в галузі безпеки підприємництва, погоджуються, що під інформаційною безпекою необхідно розуміти стан захищеності інформаційного середовища суспільства, забезпечуючи її формування і розвиток в інтересах громадян, організації і держави [58, *260–264*].

Безпечний інформаційний обмін всередині підприємства і з його зовнішнім середовищем може бути забезпечений шляхом проведення цілеспрямованих превентивних дій на зниження рівня відтоку відомостей і впровадження у практику відповідних механізмів захисту інформаційних ресурсів від зовнішніх і внутрішніх загроз. Інформаційні ресурси — це інформація з обмеженим доступом, що становить банківську і комерційну таємниці; інформація, віднесена до категорії державної таємниці, конфіденційна інформація тощо.

Для системної побудови загальної структури захисту інформаційних ресурсів підприємства застосовуються системний підхід (стратегія), системний аналіз (тактика), функціонально-вартісний аналіз, комплексний підхід. Нагадаємо, що система сприймається як комплекс елементів, що знаходяться у взаємодії. До системи захисту інформаційних ресурсів підприємства входять комплекс організаційно-технічних і програмних заходів, а також методів криптографії [51, *53–54*].

Ми поділяємо погляди переважної більшості авторів розробок, в яких розглядаються проблеми інформаційної безпеки, що необхідність захисту інформації, як правило, виникає:

- при роботі виконавців з конфіденційними документами і відомостями;
- в процесі традиційного документообігу;
- при обробці інформації в автоматизованих системах;
- при обробці інформації, що зберігається і передається у локальних мережах;
- при передачі інформації каналами зв'язку;
- при веденні конфіденційних переговорів.

Використання підприємницькими структурами різноманітних методів комерційного шпигунства здавна було одним з найефективніших методів вирішення проблеми, пов'язаної з досягненням неправомірних переваг за умов конкурентної боротьби і отриманням максимально можливого прибутку.

Багаторічна практика отримання доступу до економічних і промислових секретів конкурентів і конфіденційних відомостей комерційного характеру неодноразово засвідчувала, що це ефективний засіб користування достовірною інформацією в усіх галузях ринкової економіки [83].

Досягненню поставленої мети сприяє правильно обрана тактика дій, націлених на отримання відомостей за умов обмеженого до них доступу. Для діяльності злочинців характерне застосування різноманітних методів та новітніх інформаційних технологій, що впливають на збереження комерційної інформації і потребують вживати адекватних заходів [79].

Технічний аспект проблеми захисту підприємницької інформації висуває на перший план завдання застосовувати сучасні науково-технічні засоби захисту відомостей, що зберігаються на конкретних носіях [77].

На сьогодні це завдання ще не можна вважати розв'язаним, незважаючи на відомі успіхи, оскільки застосування найсучасніших технологічних пристроїв і приборів для захисту таємниць підприємства лише стримує їх відтік. Не має сумнівів, що незначна, на перший погляд, інформація при значних обсягах забезпечує перехід кількості в якість за належного ототожнення та аналітичного опрацювання.

Забезпечення успішної комерційної діяльності будь-якого підприємства полягає не лише у захисті таємної підприємницької інформації, а й передбачає збирання, аналіз, оцінку і прогнозування [78].

Саме збирання відомостей дає змогу на основі застосування науково розробленої системи методів пояснити суть виявлених процесів, пов'язаних з економічним становищем конкурента, виробити реакцію на вплив ситуації, подумки сформувати прогностичну модель найоптимальніших способів дій і межі поведінки в процесі використання інформації [35, *12–19*].

Тут доречно звернути увагу, що інформація цінною є лише тоді, коли може бути використаною споживачем. Особливе місце в арсеналі засобів захисту конфіденційної інформації, що обертається в процесі управління організацією, належить інфраструктурі системи інформаційної безпеки. В зв'язку з цим необхідно пояснити, що вважається об'єктами інформаційної безпеки. Якщо враховувати, що в будь-якій організації, покликаної досягати поставленої мети, інформаційні процеси реалізуються в традиційному або автоматизованому режимах, то до об'єктів інформаційної безпеки, як правило, відносять матеріально-технічні засоби інформатизації, інформаційні ресурси з обмеженим доступом, споживачів і персонал.

Щодо інформаційної безпеки. На відміну від інших видів діяльності тут об'єктом захисту стає інформаційний ресурс, тобто інформація на матеріальних носіях, серед яких, наприклад, можна назвати технічну документацію, документи, бази даних і т. д.

Право на доступ до інформаційного ресурсу юридично закріплено за його власником, ним же регулюється порядок доступу, використання, зберігання і переміщення інформації. На наш погляд, до об'єктів інформаційної безпеки можуть бути віднесені не лише матеріальні об'єкти, але і процеси, наприклад, запровадження спеціального діловодства для конфіденційних документів, надання права на користування таємною інформацією, документальне оформлення доступу до конфіденційної інформації підприємства тощо.

До методологічних основ інформаційної безпеки належить її понятійний апарат і структура, що відображає будову і внутрішню форму системи інформаційної безпеки підприємницької діяльності, і, що найсуттєвіше, загальні принципи створення і роботи системи захисту інформації господарюючого суб'єкта.

Для характеристики інформаційної безпеки суттєве значення мають наведені у працях багатьох вчених різні погляди та принципи, які покладені ними в основу пізнання на теоретичному рівні діяльності, пов'язаної з захистом інформації.

"Захист інформації у сфері бізнесу — це гарантія охорони прав власності на інформацію, яка належить конкретній особі і має майнову цінність, пов'язану з секретністю, — розмірковує

над цим П. М. Клименко. — Секретність стає одним із засобів охорони інформації”*.

В інформаційно-довідковому посібнику “Організація і сучасні методи захисту інформації”, підготовленому авторським колективом за редакцією С. Н. Дієва, проаналізовано нинішню практику захисту інформації у сфері підприємницької діяльності. Автори посібника називають відсутність порушень секретності і цілісності інформації — безпекою інформації. Виявляється, визначення інформаційної безпеки повинно відображати її природу, основний зміст і місце в системі захисту підприємства.

Спираючись на це, можна запропонувати модифіковане визначення інформаційної безпеки підприємницької діяльності як стан захищеності інформаційних ресурсів, технологій їх формування і використання, а також прав суб’єктів на інформаційну діяльність, що виключає порушення таємності і цілісності інформації.

Зважаючи на можливі загрози інформаційній безпеці, можна стверджувати, що види діяльності людей, які забезпечують процес захисту інформації, багатосторонні. Як відомо, джерелом умисних загроз при застосуванні різноманітних технологій обробки інформації в кінцевому випадку є людина [36, *34–36*].

Розглянемо з позиції системного підходу з урахуванням пріоритету загрози усі складові системи інформаційної безпеки. Вибір порушником тієї чи іншої форми атаки на інформацію здійснюється з урахуванням існуючих на об’єкті посягання технологій обробки інформації. Необхідно мати на увазі, що вибір злочинцем способів і хитрощів є не випадковим, а багато в чому залежить від мети злочинного посягання, рівня підготовки і можливостей виконавця, прогнозованої обстановки, в якій йому доведеться діяти [60].

Диференційований аналіз зв’язку протиправних посягань у сфері конфіденційної інформації з реальними можливостями осіб, які мають намір заволодіти комерційними секретами, доз-

---

* П. М. Клименко. Інформація як об’єкт інтелектуальної власності, що потребує охорони // Недержавна система безпеки підприємництва як суб’єкт національної безпеки України: Зб. наук. праць. Київ, 16–17 травня 2001 р. — К.: Вид-во Європейського ун-ту, 2003. — 287 с.

воляє виявити і конкретні види правопорушників, що посягають на інформаційну безпеку господарюючого суб'єкта.

На наш погляд, ними можуть бути:

- співробітник служби безпеки господарюючого суб'єкта;
- співробітник підприємства, що має доступ до особливо важливих виділених приміщень;
- людина, яка знаходиться за межами контрольованої зони, організованої шляхом створення замкнутих, обладнаних технічними засобами спостереження, рубежів загрози порушенню безпеки;
- людина, яка перебуває в межах контрольованої зони, але без доступу у виділені приміщення;
- людина, яка має доступ до виділених приміщень і працює в них.

Достатнє уявлення про загрози інформаційній безпеці і види правопорушників дозволяє співробітникам служби безпеки підприємства своєчасно вживати відповідних заходів щодо захисту від можливих "атак" на об'єкти інформаційної системи. Під час їх розробки не можна не враховувати основні елементи, а саме: об'єкти інформаційного захисту і види правопорушників (їхні потенційні можливості, характер, поле діяльності). Саме такий аналіз є передумовою для матеріалістичного пояснення сутності основних характеристик структурних компонентів, цілеспрямованої системи захисту інформації, що обертається в організації та її зовнішньому середовищі.

Найважливішими структурними елементами системи захисту інформації, пов'язаними взаємними відносинами, можна вважати такі засоби захисту:

- фізичні;
- адміністративні;
- апаратні;
- програмні;
- криптографічні;
- атестація системи комп'ютерної безпеки.

Вони широко використовуються для досягнення таких цілей:

- усунення несанкціонованого доступу до документів і комп'ютерної інформації через технічні канали, що створюються засобами обчислювальної техніки, і програмне забезпечення;

- запобігання знищенню інформації або несанкціонованої її модифікації;
- протидії незаконному заволодінню конфіденційною інформацією через матеріально речові канали (викрадення зразків виробів, копіювання, фотографування документів, креслень);
- протидії вивідуванню відомостей у співробітників, яким інформація була довірена;
- протидії незаконному заволодінню конфіденційною інформацією через візуально оптичні, акустичні канали [58, *289–294*].

Останнім часом значна увага приділяється питанням забезпечення інформаційної безпеки в корпоративних, міжкорпоративних мережах платіжних та інших автоматизованих систем. Фізичні засоби захисту інформаційних систем можуть бути різноманітними та їх вибір залежить від вирішуваних за їх допомогою завдань, характеру носія інформації, методів обробки інформації з обмеженим доступом та каналів передачі даних.

Фізичні засоби захисту, як правило, застосовуються для забезпечення виконання таких завдань: протипожежного захисту приміщень, в яких розміщується обладнання системи опрацювання інформації або обчислювального центру; протидії проникненню правопорушників у виділені приміщення ОЦ шляхом зміцнення дверей, вікон, блокування попереджувальної електросигналізації приміщення ОЦ, центру обробки інформації та інших вразливих місць захищених об'єктів; контролю за доступом співробітників у приміщення ОЦ чи центру обробки інформації; контролю за дотриманням персоналом встановленого на підприємстві режиму праці.

Програмні засоби — це спеціальні програми, що входять до складу програмного забезпечення системи обробки інформації для попередження несанкціонованого передавання даних через локальну мережу чи Інтернет, викликаної TEMPEST атакою, а також протидії перехопленню композитного сигналу монітора.

TEMPEST — атака здійснюється шляхом "зараження" потрібного комп'ютера спеціальною програмою-закладкою ("троянській кінь") чи іншими засобами (наприклад, з використанням технологій побудови комп'ютерних вірусів: через компакт-диск з презентацією, цікавою програмою, через диске-

ту з драйверами, а якщо персональний комп'ютер підключений до локальної мережі, то і через неї) [85]. Впроваджена програма дає можливість передавати інформацію шляхом програмного управління випромінюваннями комп'ютера. І що суттєво, програма-закладка шукає необхідну інформацію на дискові, за допомогою різних пристроїв комп'ютера, викликаючи появу побічного випромінення. Перехоплення випромінення центрального процесора за допомогою розвідувального приймача дозволяє одержати інформацію безпосередньо через підключення до комп'ютерної системи.

Серед програмних засобів захисту широкого застосування набувають антивірусні програми, засоби, що мінімізують високочастотні випромінення, зокрема, Tempest-шрифти.

Методи технічного захисту інформації входять до складу програми Tempest-захисту і застосовуються для виконання функцій запобігання відтоку таємної інформації шляхом перехоплення технічними засобами розвідки електромагнітних випромінень комп'ютера. З цією метою застосовують, як правило, пасивний метод попередження відтоку даних, що обробляються в електронному вигляді, через технічні канали.

Пасивний метод — це сполучення екранування корпусу і окремих елементів комп'ютера з застосуванням високочастотних фільтрів з тим, щоб досягти великого затухання в широкому діапазоні частот.

Завдання попередження можливості перехоплення електромагнітних випромінень в інформаційних системах, базовим елементом яких є комп'ютер, вирішуються переважно за допомогою спеціальних широкосмугових джерел шуму, функціонування яких робить неможливим застосування закладених для підслуховування пристроїв (так званий активний метод захисту інформації).

Інший варіант захисту інформації — екранування джерела випромінення комп'ютера для зменшення рівня випромінення робочої станції. Практики радять розміщувати його у сталевій шафі чи в екранованому приміщені.

Нині комп'ютери випускають у захищеному від відтоку інформації через канали ПЕМВН виконанні.

Особливе значення для захисту інформації в локальних обчислювальних мережах мають технології, засновані на напилен-

ні спеціальних матеріалів на внутрішню поверхню корпусу комп'ютера з метою знизити рівень сигналу, що випромінюється робочою станцією [39, *104–108*].

На сьогодні існує безліч електронних, електронно-механічних пристроїв, апаратних засобів, конструкторсько-технологічних, схемотехнічних рішень, направлених на попередження відтоку інформації через технічні канали у персональних комп'ютерах. Назвемо деякі з них: екранування провідних комунікацій з метою попередити відтік інформації в ланцюгах електроживлення і заземлення; використання перешкодно подавляючих фільтрів, що дають можливість знизити кондуктивні перешкоди від зовнішніх та внутрішніх джерел перешкод; уникнення впливу зміни напруги в мережі на роботу комп'ютера шляхом застосування пристроїв погодження з мережею електроживлення, однією з функцій яких є фільтрація високочастотних коливань у ланцюгу захисту заземлення корпусу комп'ютера; вибір і використання такого схемотехнічного рішення захисного заземлення обчислювальної системи, яке відповідає вимогам техніки безпеки і не погіршує властивостей усього екранованого об'єкта, на якому розгорнута локальна мережа, тощо.

Зрозуміло, застосування технічних засобів захисту інформації в жодному разі не замінює собою спеціаліста, який контролює сигнали, отримані за допомогою відповідних електронних пристроїв, у разі порушення рубежів захисту.

В останні роки з'явилася можливість підійти до вивчення проблеми захисту підприємницької інформації комплексно, оскільки переважна більшість опублікованих робіт присвячена або конкретним системам захисту інформації, або її окремим аспектам [73].

Наші уявлення про інформаційну безпеку дедалі поглиблюються. Однак принципове значення має правильне розуміння меж захищеності підприємницької інформації та фізико-технічних основ, спеціально розроблених технічних засобів і винайдених тактичних прийомів.

Одну з головних ролей у забезпеченні інформаційної безпеки підприємств різних організаційно-правових форм (малих підприємств, науково-виробничих об'єднань, фінансово кредитних установ і т. д.) відіграють принципи організації системи захисту

комерційної таємниці, методики комплексного контролю і перевірки захищеності інформації, якісний аналіз основних завдань захисту інформації [17].

Зазначимо, що практична реалізація організаційних заходів стосовно захисту підприємницької інформації неможлива без вирішення деяких ключових питань, серед яких можна виділити:

- доступ до інформації, що вважається комерційною таємницею;
- створення надійного захисту засекреченої інформації її власником або уповноваженим ним органом;
- комплексний контроль за захищеністю інформації, що є власністю підприємства.

Робота щодо захисту інформації на підприємстві головним чином пов'язана з протидією несанкціонованому отриманню інформації за допомогою технічних засобів розвідки. Пояснимо це на прикладі. Якщо два співробітники підприємства ведуть ділову розмову у виділеному приміщені, то обмін вербальною інформацією між ними відбувається у повітряному середовищі. Цілком очевидно, що правопорушники, перебуваючи за межами кімнати, завчасно вибрали вигідну позицію для спостереження, скажімо, через вікно, за співрозмовниками. Отже, за допомогою оптичних пристроїв посилення зору (за артикуляцією губ) вони можуть отримати потрібну інформацію.

Здавалося б, до передачі захищеної інформації через різні канали має стосунок лише основне середовище, в якому поширюються сигнали, що несуть інформацію. Насправді ж, окрім основного середовища, яким виступає повітряний простір, існує ще кілька побічних середовищ передачі інформації. Наприклад, має місце так званий ефект вібрації віконного скла з частотою розмови. Наявність вібрації має вирішальне значення для вибору конкретного методу перетворення цих механічних коливань у гучну розмову.

Постає питання: чи існує зв'язок між характеристиками акустичних сигналів, що виникають під час розмови у приміщенні, і методами відтворення мовної інформації, що переказується?

Розглянемо відтворення як процес повторного отримання інформації, що передається у вигляді акустичних сигналів і не за-

знала якихось суттєвих змін у побічному середовищі. Під час цього процесу відображеним є джерело інформації, наприклад, людина, а відображаючим — технічна система, що дає змогу зчитувати вібрацію з вікон і перетворювати її в розмову.

Необхідно зазначити, що для прослуховування приміщення нині використовують, зокрема, лазерні мікрофони. Тому на вікно завчасно наносять пляму фарби, що відбиває лазерний промінь на випромінювач, де за допомогою фотодіодного пристрою здійснюється перетворення світлових коливань у електричні.

На практиці вирішення питань організації на підприємствах різноманітних систем захисту таємної підприємницької інформації потребує створення рубежів захисту за межами контрольованих зон. Об'єктами захисту в межах таких територій, як правило, виступають операційні зали, кімнати — сховища комп'ютерної інформації, особливо важливі виділені приміщення, в яких розміщено сейфи з таємною інформацією, тощо [82].

Використання рубіжної системи захисту підприємницької інформації не випадкове, а зумовлене тим, що саме вона дає змогу забезпечити безпеку при реалізації різноманітних технологій обробки таємної інформації шляхом тотального контролю.

Носієм інформації в традиційному вигляді виступає документ, який в управлінській діяльності визначається як матеріальний об'єкт з інформацією, що закріплена створеним людиною способом для її передачі у часі і просторі [89]. За способом фіксації інформації документи поділяються на письмові, графічні, фото -, фоно -, відео- і кіно документи.

Письмові — усі рукописні тексти і машинописні документи, виготовлені з використанням різноманітних друкованих пристроїв і друкарським способом.

До графічних відносяться малюнки, плани, схеми, креслення, графіки, карти.

Фонодокументи — звукозаписи інформації, що широко використовується при складанні протоколів зборів, нарад, засідань і т. п.

Дискети — носі інформації в електронному вигляді.

Як відомо, інформація людям передається через відчуття: зір, слух, смак.

Важливою характеристикою інформації є формат, сприйнятливий як людиною, так і ЕОМ. Люди отримують більшу частину

інформації у вигляді записаного (зображеного) матеріалу або у вигляді документації.

Відповідно до сьогоднішніх уявлень, інформація завжди себе проявляє в матеріально-енергетичній формі. Річ у тім, що обмін інформацією вбудований у всі види управлінської діяльності і відбувається завдяки використанню різних фізичних явищ і способів. У теорії управління ці процеси дістали назву комунікативних процесів зв'язку.

Зазначимо, що кожному способу обміну інформації притаманне своє основне середовище. Існують і побічні середовища, вони зберігають відображену інформацію, тобто джерело інформації.

Нам, насамперед, важливо зрозуміти співвідношення основного і побічного середовищ в обміні інформацією. Розглянемо це на прикладі роботи користувача персонального комп'ютера з монітором. Відомо, що монітор створено для візуального відображення інформації.

Користувач персонального комп'ютера отримує інформацію у вигляді композитного сигналу монітора, що являє собою змінені в певній послідовності електричні і магнітні поля. Інформація візуально відображається на екрані монітора. Легко зрозуміти, що в даному випадку основним середовищем обміну інформацією є видима частина спектра електромагнітних коливань.

Як уже зазначалося, при роботі монітора існують і побічні середовища, що містять відображену інформацію. Розглянемо їх детальніше. В процесі функціонування монітора його багаточисленні електронні схеми створюють електромагнітне випромінення в діапазоні до 100 Мгц, а електронно-променева трубка викликає рентгенівське випромінення.

Рентгенівські промені — це електромагнітні хвилі. За своїми якостями вони примикають до спектра видимих променів, але більша їх частина людським оком не сприймається.

Побічні електромагнітні випромінення відеомоніторів і їх елементів, що несуть таємну інформацію, можуть бути перехоплені за допомогою засобів радіо- і радіотехнічної розвідки кримінальними і конкурентними комерційними структурами [58, *244*].

Перехоплення і декодування побічних електромагнітних випромінень, що створюються конструктивними елементами ПК, наприклад, монітором і клавіатурою, являють собою серйозну загрозу захисту комерційних таємниць за автоматизованої обробки інформації.

Суб'єктом управління системою захисту інформації, що опрацьовується на об'єктах електронно-обчислювальної техніки того чи іншого підприємства, є служба безпеки.

Необхідно звернути увагу, що на сьогодні роботи з захисту інформації, що обертається в комп'ютерах і комп'ютерних мережах, проводиться в чотирьох основних напрямах:

- протидія несанкціонованому доступу до інформаційних потоків підприємства за допомогою програмного забезпечення і засобів інженерно-технічної розвідки;
- оптимізація організаційних і організаційно-технічних заходів опрацювання конфіденційної інформації з метою попередження її викрадення, знищення;
- блокування несанкціонованого доступу до зберігання і опрацювання інформації за допомогою засобів обчислювальної техніки, що передається через лінії зв'язку абонентів;
- попередження несанкціонованої модифікації інформації.

Не можна не погодитись з наведеною у літературі думкою, що підприємницька інформація має різні форми зберігання, серед них найпоширенішими є людська мова, документи, машинні носії (жорсткі диски). Це й зумовило застосування різних способів її передачі, зберігання і обробки.

При організації захисту інформації з обмеженим доступом, що обробляється на персональних комп'ютерах, необхідно враховувати ті чи інші фізичні явища, характерні для форм її зберігання на об'єктах ЕОМ.

Залежно від фізичної природи виникнення і середовища поширення паразитних випромінень і наведень технічні канали відтоку інформації в комп'ютерній мережі поділяють на електромагнітні, параметричні та електричні [39, *104–108*].

Відомо, що класифікація — це перший крок до пізнання законодавчої норми. Наступні дослідження загальної теорії захисту інформації, вивчення її фундаментальних основ веде до глибшого розуміння запропонованої в літературі свого часу лише емпіричної класифікації технічних каналів відтоку інформації.

За останні п'ять-шість років простежується значне посилення уваги до теоретичних і практичних питань захисту інформації, що опрацьовується на об'єктах електронно-обчислювальної техніки. Вони знайшли своє відображення у колективному інформаційно-довідковому посібнику "Організація і сучасні методи захисту інформації", а також у роботах С. Коженевського, А. Мурашова, С. Прокопенко, А. Провозіна, С. Чеховського, Л. Козленко та ін. [39, *104–108*].

В роботах, присвячених проблемі інформаційної безпеки, значна увага приділяється відновленню і гарантованому знищенню відомостей, що зберігаються на жорстких дисках, попередженню відтоку інформації через електромагнітне випромінення і наведення при опрацюванні на персональному комп'ютері. Однак питання про тактичний характер вибору ефективних заходів протидії посяганням в комп'ютерних мережах, адекватних тим спеціальним методам і засобам, якими може скористатися правопорушник, розвитку не отримало і, на наш погляд, залишилося поза увагою спеціалістів у цій галузі.

При оцінці доцільності вибору того чи іншого спеціального методу і засобу, необхідних для контролю за випромінення комп'ютера і захисту від відтоку інформації, що у ньому опрацьовується, не може перевищувати значення в цьому логічному процесі сутності фізичних явищ, що відбуваються при виникненні каналів відтоку. Вирішити це правильно дозволить лише облік деяких інших, не менш важливих, критеріїв. Серед них можна назвати загальні умови раціонального використання наявних технічних можливостей і фактори впливу на ефективність дій щодо захисту інформації в системах, де базовим елементом є комп'ютер.

Вирішення питання про використання правопорушником тих чи інших спеціальних методів і засобів для виявлення і перехоплення сигналу з конфіденційною інформацією пов'язано не лише з чітким знанням фізичних явищ, характерних для різних форм зберігання інформації на об'єкті електронно-обчислювальної техніки, а й з визначенням спеціальних методів, застосованих для блокування "небезпечного" сигналу і закриття каналів відтоку інформації.

Складність щодо незаконного отримання конфіденційної інформації конкурента за допомогою технічних засобів розвідки

має об'єктивний характер. Це пояснюється, зокрема, тим, що не всі технічні канали відтоку інформації формуються лише за рахунок електромагнітного випромінення і наведень, що модулюються сигналами, які виникають у комп'ютері під час обробленя інформації. Має місце й штучне створення людиною технічних каналів відтоку інформації шляхом встановлення в комп'ютері або мережі електроживлення радіотрансляторів (закладок), чи через високочастотне нав'язування. Скажімо, у кабелі, що виходять за межі контрольованих зон, кабелі мереж електроживлення, заземлення комп'ютера і периферійних пристроїв вводять, так званим контактним способом, струми високої частоти. Високочастотні струми, що подаються через мережу електроживлення на нелінійні елементи, призводять до виникнення комбінаційних частот, що відображаються і приймаються за допомогою спеціального обладнання і декодуються. Причому прийняті контрольним приймачем електронно-магнітні коливання будуть вже промодульовані інформаційними сигналами, опрацьованими в комп'ютері.

Особливе значення має той факт, що в автономних комп'ютерах здійснюється лише оброблення і зберігання інформації. При виділеному підключенні комп'ютера до локальної мережі або до глобальної мережі Інтернет проводяться усі види робіт з інформацією: її зберігання, оброблення і передача. Слід зазначити, що на сьогодні комп'ютер частіше використовується у локальній мережі. Тому проблеми захисту комп'ютерів від відтоку інформації через канали побічних електромагнітних випромінень і наведень необхідно вирішувати, керуючись саме цим.

Розглянемо тепер питання про виникнення "небезпечних" випромінень комп'ютера. Сучасні уявлення про комп'ютер як об'єкт технічного захисту інформації цілком пояснюють це явище. Наявність серед комплектуючих пристроїв персонального комп'ютера різноманітних за функціональним призначенням елементів викликає під час їх роботи побічні випромінення.

Як канали відтоку інформації, що опрацьовується в комп'ютерній мережі, використовують побічні електромагнітні випромінення і наведення більшості елементів самого комп'ютера — принтера, клавіатури, системного блока, акустичної системи, монітора.

Усі елементи локальної обчислювальної мережі пов'язані між собою проводами і кабелями електроживлення. Що можна сказати з приводу кабельної мережі? Перш за все вона відіграє роль антени для побічних випромінень комп'ютера і сервера. Крім того, через проводи кабельної системи в комп'ютер проникають високочастотні електромагнітні коливання, що випромінюються активним електронним обладнанням локальної обчислювальної мережі і можуть викликати додаткові випромінення в ефір на комбінаційних частотах. Зазначимо, що комбінаційні частоти виникають внаслідок впливу випромінення двох будь-яких комплектуючих пристроїв комп'ютера на елементи, вузли, блоки нелінійного перетворення сигналів з широким спектром частот.

Розглянемо обставини об'єктивного характеру, що сприяють формуванню каналів відтоку інформації через мережу електроживлення.

Для електроживлення комп'ютера, як правило, використовують промислову мережу змінного струму — 50 Гц. Загальними пристроями електроживлення є мережевий фільтр і джерело безперервного струму.

Розподіл електроживлення для окремих пристроїв персонального комп'ютера має свої особливості і здійснюється так. Електричний струм на сканер, принтер, акустичну систему подається через адаптери, конструктивно виконані як автономні пристрої. Адаптер використовується для того, щоб перетворювати змінну напругу 220 В у постійну 12 В. Поряд з автономними адаптерами в схемі електроживлення комп'ютера існують і вбудовані перетворювачі. Живлення пристроїв системного блока, клавіатури і маніпулятора (миші) від мережі змінного струму з частотою 50 Гц і напругою 220 В здійснюється через багатоканальний блок вторинного живлення. Конструктивно блок вторинного живлення вбудований у металевий кожух, в якому розміщено системний блок з пристроями обробки і зберігання інформації.

Електроживлення на принтер подається від первинної мережі (220 В, 50 Гц) через мережевий фільтр або від джерела безперервного живлення.

Для зниження рівня паразитного електромагнітного випромінення, що проникає у мережу електроживлення персонально-

го комп'ютера, застосовують мережеві перешкодоусуваючі фільтри. Звернемо увагу, що в промисловій мережі змінної напруги 220 В, 50 Гц, яку використовують для електроживлення персональних комп'ютерів, існують зміни напруги, що називаються мережевими перешкодами.

Під час роботи джерела вторинного електроживлення системного блоку виникають побічні випромінення у вигляді електромагнітних коливань. До складу блока вторинного електроживлення входять різні конструктивні елементи — контури, електричні ланцюги, дроселі, магнітні проводи. Багатоканальний блок вторинного електроживлення, що входить у схему електроживлення персонального комп'ютера, є загальним джерелом для системного блока і периферійних пристроїв. Багатоканальний блок вторинного живлення, вбудований у корпус системного блока, отримує електричне живлення безпосередньо від первинної мережі. Відзначимо, що джерела живлення слугують проміжною ланкою між первинною електромережею і вузлами комп'ютерів, тому вони мають бути нібито фільтрами, тобто не передавати перешкоди з мережі у навантаження.

Необхідно зазначити, що під час роботи автономні і вбудовані перетворювачі змінної напруги — 220 В у постійну 12 В — створюють паразитні контури. Наприклад, автономні перетворювачі створюють такі паразитні контури, як: первинна мережа — вхід адаптера, вихід адаптера — навантаження; а вбудовані перетворювачі: первинна мережа — перетворювач — навантаження. Слід пам'ятати, що додатковий паразитний контур створює ланцюг електроживлення принтера.

Усі паразитні контури від різних пристроїв мають загальну точку, що через ланцюг первинного електроживлення з'єднана з пристроями за межами контрольованої зони. Загальне джерело вторинного електроживлення для пристроїв системного блока ПК створюють серйозні ускладнення для вирішення завдань розподілу паразитних контурів.

Дуже важливе значення мають фактори, що обумовлюють поширення побічних випромінень як у самому джерелі вторинного електроживлення системного блока персонального комп'ютера, так і в проводах, що подають змінну напругу 220 В з частотою 50 Гц.

Причинами виникнення перешкод у пристроях комп'ютера є: паразитні ємнісні й індуктивні зв'язки між інтегральними схемами у ланцюгах електроживлення і контурах заземлення; комутаційні процеси, що виникають при перемиканні транзисторів-перетворювачів змінної напруги — 220 В у постійну 12 В; перехресні наведення між сигнальними лініями через паразитні ємності та індуктивності; наведення від зовнішніх електромагнітних полів.

Під перешкодами у ланцюгах електроживлення комп'ютера вважаються побічні електромагнітні випромінення, що йдуть від джерела перешкод до приймача перешкод двома способами: кондуктивним, тобто через прохідні ланцюги, і випромінением через простір.

Середовищем поширення електромагнітних перешкод є: простір з побічними електромагнітними випромінюваннями; металеві частини корпусів, вузлів і блоків; паразитні ланцюги монтажу; паразитні міжобмоткові ємності розподільчих трансформаторів; міжвиткові ємності дроселів фільтрів; різноманітна з'єднувальна проводка; джерело живлення і заземлений контур; ланцюги електроживлення. З сучасної фізики відомо, що всі закономірності керуються чотирма типами взаємодії:

- електромагнітними;
- гравітаційними;
- слабкими;
- сильними.

Не можна зрозуміти фізичну сутність каналів відтоку інформації, що обертається у комп'ютері і комп'ютерних мережах, без розуміння процесів випромінення елементів комп'ютера, випромінення на комбінаційних частотах, високочастотного нав'язування, мікрофонного ефекту і факторів, що сприяють негативному впливу на інформаційні потоки.

Серед умов для формування технічних каналів відтоку інформації через ланцюги електроживлення можна назвати такі обставини: неоптимізовану кількість паразитних контурів, наявність у паразитних контурів загальної точки, що забезпечує взаємний обмін побічними електромагнітними коливаннями; безліч видів побічних коливань багатоканального блока вторинного живлення.

Слід також мати на увазі таке: побічні коливання можуть бути промодульовані, по-перше, сигналами, що формуються під час автоматизованої обробки інформації комп'ютером, і по-друге, голосовою інформацією (акустичним полем), оскільки деякі конструктивні елементи електричного пристрою мають мікрофонний ефект. А це означає, що промодульовані побічні коливання можна перехопити, виділивши не лише дані, що обробляються у комп'ютері, а й прослуховувати приміщення.

Характеризуючи обставини, що сприяють формуванню каналів відтоку інформації, необхідно враховувати і багатопланові фактори, від яких залежить можливість перехоплення побічних електромагнітних випромінень комп'ютера.

Річ у тім, що кожному фізичному явищу відповідає безліч параметрів, зміна яких визначає сигнали середовища, в якому відбувається обмін інформацією.

Для кожного виду загроз безпеці підприємницької інформації необхідно використовувати різні за змістом заходи протидії отриманню секретної інформації [81].

Виходячи з вимог безпеки інформації, що зберігається, необхідно здійснювати заходи з використанням різних технологій і засобів захисту. Пошук радіоелектронних засобів несанкціонованого знімання інформації поетапний:

- вивчення службою безпеки підприємства оперативної обстановки біля об'єкта інформації;
- перевірка радіоефіру за межами приміщення;
- перевірка моніторингу радіоефіру у приміщені за допомогою нелінійних локаторів у діапазоні частот 0,1–2000 МГц;
- перевірка комп'ютерів, телефонних апаратів, електротехнічних засобів за допомогою скануючого приймача;
- перевірка стін приміщення за допомогою діапазонного скануючого приймача або індикаторів поля;
- обстеження меблів та інших предметів у приміщені за допомогою детектора випромінювання;
- перевірка телефонної та електронної ліній за допомогою комплексу "Scanner 99".

Серед наявних нині засобів забезпечення безпеки інформаційних систем можна навести конкретний їх перелік: технічні, спостереження, контроль, ідентифікація та інші.

Технічне забезпечення захисту конфіденційної інформації передбачає:

- категоріювання об'єктів, що мають комп'ютерні системи;
- обстеження службою інформаційної безпеки підприємства об'єктів, на яких використовуються комп'ютерні технології (до служби інформаційної безпеки підприємств, установ, організацій належать: керівник установи, системний адміністратор чи системний програміст, керівник служби безпеки підприємства, аудитор, спеціаліст інформаційної системи);
- атестування системи комп'ютерної безпеки з метою підтвердити відповідність вимогам стандарту безпеки інформації;
- технічний контроль за спеціальною апаратурою, що використовується для забезпечення безпеки і таємності інформації.

До секретної інформації відносять таку, що не підлягає розголошенню через її корисність для підприємницької діяльності, має справжню чи потенційну цінність матеріального або нематеріального характеру і є недоступною для конкурентів, забезпечуючи власникові переваги у комерційній або іншій діяльності.

Перевірка партнерів у підприємницькій діяльності — це вжиття, так би мовити, превентивних заходів у боротьбі з комерційним шпигунством та недобросовісною конкуренцією [62].

Встановлення останнім часом принципово нових відносин між суб'єктами господарської діяльності, діяльність бізнесу за умов економічного ризику потребує від суб'єктів господарської діяльності використання певних масивів інформації для прийняття того або іншого рішення [10].

При укладанні договорів важливе значення має наявність у контрагентів необхідних свідчень про надійність потенційного партнера підприємницької діяльності, щоб мінімізувати ризики, адже у сфері підприємництва часто вдаються до шахрайства.

Практика свідчить, що ризики зводяться до мінімуму на тому підприємстві, де створена організаційна система перевірки надійності комерційних партнерів, яка за допомогою правомір-

них методів збирає інформацію про майбутнього партнера з зовнішнього середовища.

Можна звернути увагу на правову неврегульованість цього питання. На практиці комерційні служби безпеки часто не звертають уваги на тонкощі законодавства України та гарантовані Конституцією права і свободи громадян. Іноді неправомірні дії служб безпеки підприємств є підставою для притягнення до кримінальної відповідальності, скажімо, за ст. 359 КК України (незаконне використання спеціальних технічних засобів негласного отримання інформації) та ст. 182 (порушення недоторканності приватного життя) [1].

У зв'язку з цим необхідно розглянути сучасні методи перевірки надійності недобросовісних контрагентів, які приховують свої наміри не виконувати обов'язки згідно з договором.

Різновидами шахрайства є використання вигаданих даних (несправжнього імені, неправдивої адреси) при укладанні, наприклад, договору про передачу продукції на реалізацію. Використання підроблених, викрадених, втрачених документів законних власників також вважається шахрайськими діями.

У юридичній літературі більшість авторів вважає, що насамперед слід упевнитися, чи особа, яка збирається підписати договір, має на це певні права. Необхідно чітко уявляти, хто веде з вам переговори, чи є у контрагента право підписувати договір. Тому треба не соромитися перевірити паспорт чи інший документ, що засвідчує особу.

Під час попередніх переговорів слід ознайомитися з документом, що підтверджує повноваження особи на підписання попередніх договірних документів та укладання самого договору, а саме зі Статутом підприємства. Справді, чи можна уявити собі методику перевірки повноважної особи, яка підписує договір, не отримавши даних про його компетенцію, право не тільки брати участь у переговорах, а й приймати рішення з конкретних питань від імені контрагента.

На практиці може мати місце таке, коли директор працює за наймом, в власники підприємства певною мірою обмежують його повноваження щодо розпорядження майном і надають їх тільки за згодою ради директорів. У таких випадках у статуті підприємства, у розділі "Компетенція директора" вказується, що директор має право укладати договори на суму, скажімо,

більшою від 100000 грн. лише за згодою Адміністративної ради підприємства.

Слід також пам'ятати, що лише перший керівник має право виступати від імені підприємства без доручення. Про це можна дізнатися з наказу та протоколу зборів власників підприємства про права директора.

За дорученням у переговорах може брати участь заступник директора підприємства-контрагента, якому, до речі, можуть бути делеговані значні повноваження з конкретних питань. У такому випадку будь-якого особливого доручення не потрібно.

Головний бухгалтер підприємства має право укладати договори лише за наявності доручення.

Як свідчить досвід, уже на першому етапі підготовки угоди велике значення має чітка та повна фіксація фірмових назв контрагентів згідно з державним реєстром.

Оскільки йдеться про практичні дії щодо захисту грошових і товарних засобів підприємства, то зупинимося на питаннях методики перевірки особи, яка діє від імені підприємства-контрагента. Доручення — це офіційно завірений документ. Методика його перевірки полягає у такому:

- чи є на дорученні підпис керівника (обов'язково керівника!) підприємства та чи дійсна печатка;
- дата, коли видане доручення (якщо дати немає, то доручення недійсне);
- термін, на який видане доручення;
- обсяг повноважень, з яких чітко зрозуміло, що той, хто перед вами, справді має право вести переговори від імені організації чи представляти її інтереси.

Необхідно пам'ятати: угода, що укладається від імені іншої особи, є перевищенням прав, однак не тягне за собою ніяких правових наслідків до особи, від імені якої вона укладається. Водночас не треба забувати, що повноваження особи підписувати банківські документи не означає, що вона має право укласти угоду від імені підприємства.

Перевірку партнера доцільно здійснювати, спираючись на можливості служби безпеки підприємства, ставлячи перед нею конкретні завдання щодо надійності партнера, його платоспроможності, саме такі дані можуть бути використані керівни-

ком підприємства для прийняття рішення — входити у ділові стосунки чи відмовитися від партнерства.

Обов'язки служби безпеки мають полягати у збиранні, аналізі, обробці інформації про ділових партнерів, які можуть вдаватися до недобросовісної конкуренції.

Нині, за умов бурхливого розвитку підприємницької діяльності в Україні, а також у країнах близького та далекого зарубіжжя, основним джерелом такої інформації є:

- фірма "Сакура", яка надає інформацію про надійність і платоспроможність українських та світових партнерів;
- міжнародна служба безпеки "СКІФ", від якої можна отримати різнобічну інформацію як юридичним, так і фізичним особам про українські та закордонні підприємницькі структури будь-якої форми власності та виду діяльності;
- Торгово-промислова палата України, яка зібрала солідний банк даних про українські та закордонні компанії, фірми і підприємства усіх форм власності;
- підрозділ "Інформцентр" Української федерації працівників недержавної служби безпеки.

Визначення конкуренції дано в Законі України "Про захист економічної конкуренції", згідно з яким конкуренція — це змагальність підприємців, коли їх самостійні дії обмежуються можливістю впливати на загальні умови реалізації товарів на ринку та стимулюють виготовлення таких товарів, які потрібні споживачеві.

Підприємницька інформація в ринково-конкурентному середовищі поділяється на технічну, організаційну, комерційну, фінансову, рекламну про попит і пропозицію, про конкурентів і кримінальне середовище. Різноманітні потоки інформації, необхідні для функціонування підприємства, можна умовно розподілити на групи. Один потік інформації про методи і засоби захисту комерційних секретів підприємства, такі відомості зберігаються та обробляються у межах спеціалізованої оперативної системи. Другий потік — це інформація про економічне становище підприємства, зокрема про прибуток, ресурси, позитивні і негативні фактори, що впливають на розвиток комерційної діяльності, конкурентоспроможність продукції тощо. Цей інформаційний контур, що містить конфіденційні відомості діло-

вого, економічного, виробничого характеру, входить до так званої "підприємницької інформаційної системи".

До значної частини потенційної інформації відкрито вільний доступ, а саме до чинного законодавства, що регулює діяльність підприємницьких структур. Ці знання можна використати для забезпечення зберігання комерційних секретів, тому такі відомості не можна ігнорувати. Але в кожному конкретному випадку не вся інформація має комерційну таємницю.

В організації захисту комерційної таємниці підприємства є така особливість: розв'язання певного завдання або його частини доручається конкретному підрозділу чи спеціалісту.

Більше того, такий поділ праці не випадковий. Адже кожний колектив — це єдиний, цілісний організм, члени якого спільно прагнуть досягти певної мети. Зміст роботи спеціалістів, які відповідають за організацію ефективної роботи системи внутрішньої безпеки підприємства, полягає в тому, щоб серед обслуговуючого персоналу виявити тих, хто в процесі господарської або іншої діяльності виявляє підвищений інтерес до угод і партнерів, інформаційних архівів, технологічних та комерційних секретів.

Як правило, вирішення проблеми протидії викраденню інформації, що має комерційну таємницю, покладається на підрозділ режиму служби безпеки підприємства. Координація дій з планування та реалізації внутрішніх і зовнішніх заходів захисту інформаційної системи підприємства покладається на головного спеціаліста з захисту комерційної таємниці [62].

Захист комерційної таємниці пов'язаний з організацією та веденням закритого діловодства. На керівника групи закритого діловодства та головного спеціаліста з захисту комерційної таємниці покладаються такі обов'язки:

- організація закритого діловодства;
- контроль за розмноженням та розсиланням документів, що містять комерційну таємницю;
- вживати заходи щодо запобігання розголошенню комерційної таємниці;
- контроль за своєчасним, правильним визначенням та зміною грифа обмеження з встановленої на підприємстві багатоступеневої системи важливості відомостей, що мають комерційну таємницю;

- вживати певних заходів щодо запобігання втрати документів, що мають інформацію з обмеженим доступом, а також фіксувати випадки розголошення відомостей, що мають банківську, комерційну таємницю або відносяться до інформації конфіденційного характеру.

За наказом керівника підприємства співробітники служби безпеки, як правило, самостійно виявляють факти розголошення інформації з обмеженим доступом, а також грубих порушень встановлених режимних вимог [63].

Правовий захист комерційної таємниці підприємства силами лише одного підрозділу забезпечити неможливо, необхідна спільна діяльність з іншими підрозділами СБ, детективною групою, відділом кадрів тощо.

До найактуальніших для теорії та практики проблем захисту комерційної таємниці входить неврегульованість законодавством України правових відносин, що виникають під час здійснення контролюючими органами перевірок фінансово-господарської діяльності. Перш за все плутанину вносить об'єднання в одне поняття "перевірка" двох зовсім різних за своєю природою сторін діяльності контролюючих органів, виконавчої влади, уповноважених від імені держави здійснювати перевірку фінансово-господарської діяльності суб'єктів підприємництва та правоохоронних органів, які здійснюють спеціальні заходи в інтересах кримінального судочинства, державної безпеки, а не з якоюсь іншою метою. Треба нагадати, що оперативно-розшукова діяльність може здійснюватись як до порушення, так і вже в рамках порушеної кримінальної справи.

Указом Президента України "Про деякі заходи з дерегулювання підприємницької діяльності" від 23.07.98 р. № 817\08 (ст. 5) встановлено, що контролюючими органами, які мають право здійснювати планові та непланові виїзні перевірки фінансово-господарської діяльності суб'єктів підприємницької діяльності є:

а) органи державної податкової служби — в частині сплати податків та сборів [обов'язкових платежів] до бюджету;
б) митні органи — в частині сплати вхідного мита, акцизного збору, та податку на додану вартість, які проводяться у випадках ввезення (пересилання) товарів на митну територію України в момент пересікання митного кордону;

в) органи державного казначейства, державної контрольно-ревізійної служби та державної податкової служби в межах їх компетенції — у відносинах бюджетних позик та кредитів, гарантованих грошима бюджетів, цільового використання дотацій та субсидій, інших бюджетних асигнувань, грошей позабюджетних фондів, а також неналежного виконання державних контрактів, проавансованих за рахунок бюджетних коштів. У тому ж указі (ст. 6) зазначається, що рішення про виїмку документів первинного обліку, призупинку на рахунках у банках, інших фінансово-кредитних закладах, а також про заборону відчуження майна суб'єкта підприємницької діяльності у зв'язку з порушенням податкового, бюджетного або валютного законодавства можуть прийматися лише органами державної податкової служби, а у випадках визначених митним законодавством — митними органами.

Ця стаття вносить прозорість у природу перевірок та ревізій суб'єкта підприємницької діяльності контролюючими державними органами. Таким чином, можливість контролюючих органів виконавчої влади ознайомлюватися з конфіденційними відомостями або з комерційною таємницею підприємства обмежена їхньою компетенцією, визначеною чинним законодавством України.

Про надання інформації державним податковим інспекціям про рахунки та вклади окремих громадян законодавець не згадує. Тому державним податковим інспекціям можуть видаватися довідки лише про операції та рахунки підприємств чи організацій [6].

Право доступу до охоронюваних відомостей, що мають банківську та комерційну таємницю, здійснення виїмки предметів і документів, що є носіями комерційної інформації, можуть мати не тільки дізнавачі прокуратури, СБУ, міліції, а й працівники органів дізнання міліції, підрозділів кримінального розшуку, боротьби з економічними злочинами, податкової міліції.

Необхідно вказати, що виїмці підлягають тільки ті документи, що мають комерційну або банківську таємницю, оскільки саме щодо таких носіїв комерційної таємниці законом встановлено спеціальний порядок отримання відомостей. Для того щоб вилучити у підприємства, закладу, організації необхідні пред-

мети, документи виноситься постанова про проведення виїмки, котра підлягає санкціонуванню прокурором.

Особливої уваги заслуговує питання щодо правового регулювання відносин підприємства з правоохоронними органами у випадках, коли останнім необхідно отримати від учасників фінансово-господарських стосунків інформацію, що має комерційну або банківську таємницю.

Здійснення співробітниками правоохоронних органів заходів, направлених на ознайомлення з деякими категоріями інформації з режимом обмеженого доступу, напряму пов'язано зі вторгненням у сферу прав суб'єктів підприємництва на комерційну та банківську таємницю, що охороняється державою. Реалізація владних повноважень правоохоронних органів у деяких випадках пов'язана з втручанням у діяльність підприємства, комерційного банку. Але такі обставини передбачені законодавством України. Так у законі України "Про банки і банківську діяльність" наводиться досить повний перелік інформації, що становить банківську таємницю, а також органів і організацій, яким вона може бути надана.

Згідно зі ст. 52 Закону України "Про банки і банківську діяльність" довідки про операції і рахунки юридичних осіб та інших організацій видаються самим організаціям, державним податковим інспекціям з питань оподаткування, а також у випадках, передбачених законодавством, за письмовим запитом судів, органів прокуратури, служби безпеки, внутрішніх справ, Антимонопольного комітету України, Державної контрольно-ревізійної служби, аудиторських організацій, господарського суду [8].

Довідки про рахунки та вклади громадян видаються, окрім самих клієнтів і їх представників, також судам, органам прокуратури, служби безпеки, внутрішніх справ у справах, що знаходяться у їх проваджені.

Контрольні питання та завдання

1. Що є підставою розглядати в науковому плані забезпечення інформаційної безпеки підприємництва як галузь загальнотеоретичної науки безпекознавства?
2. Охарактеризуйте методологію дослідження процесів формування, функціонування, розвитку системи забезпечення інформаційної безпеки підприємництва.
3. Окресліть об'єкт і предмет навчального курсу забезпечення інформаційної безпеки підприємництва.
4. Яка роль використання інформаційних технологій у сфері підприємництва?
5. Пояснити власне бачення обставин, що впливають на можливість отримати інформацію шляхом перехоплення випромінювань комунікаційних каналів, центрального процесора, принтера, дисплея.
6. Назвіть сукупність дій з окремих напрямів захисту даних в комп'ютерній системі або мережі від незаконного перехоплення і несанкціонованого зняття інформації, що зберігається на НЖМД (накопичувач з жорсткими магнітними дисками).
7. Який існує порядок ознайомлення співробітників правоохоронних органів з деякими категоріями інформації з режимом обмеженого доступу, що становить комерційну таємницю підприємства.

Додаткове завдання

Окресліть схему основних напрямів діяльності для захисту інформації при її обробці на об'єктах ЕОМ (електронно-обчислювальні машини).

Розділ II

Нормативно-правовий і організаційний аспекти діяльності суб'єкта господарювання стосовно збереження комерційної таємниці

2.1. Законодавча база у сфері захисту комерційної таємниці

Законодавство в сфері захисту комерційної таємниці може розглядатися як система правових, корпоративних норм [63]. Законодавство — це зовнішня форма існування норм права чи сукупність законів та підзаконних нормативних актів, що регулюють відповідну групу відносин. Аналіз законодавства в сфері захисту комерційної таємниці дає можливість віднести його до окремої галузі — законодавства про підприємницьку діяльність. Вивчення правових відносин, що виникають у зв'язку з здійсненням підприємницької діяльності, як відомо, відноситься до предмета комерційного права.

Серед видів соціальних норм (соціальні норми — це норми поведінки, що встановлюються суспільством і є регулятором суспільних відносин) відомі корпоративні норми (норми громадських організацій, що визначаються, виходячи зі Статуту). Статутні положення окремих підприємств відносяться до зовнішніх форм існування норм права. Ці нормативні акти розробляються на підставі загального нормативного акта, і поширюють свою дію тільки на відносини, що виникають на підприємствах. Це нормативні акти внутрішнього характеру.

У правовому змісті неправомірне збирання та використання комерційної таємниці відноситься до однієї із груп проявів недобросовісної конкуренції [73]. Стосовно недобросовісної конкуренції необхідно звернутися до спеціального законодавства, конкретно — до Закону України " Про захист від недобросовісної конкуренції" [7]. Глибоке дослідження проявів недобросовісної

конкуренції зумовлює необхідність розкрити зміст комерційної таємниці.

У ст. 505 Цивільного Кодексу України визначається зміст поняття "комерційна таємниця" [4]. Це секретна інформація, що в цілому чи в певній формі та сукупності її складових є невідомою та не легкодоступною, у зв'язку з цим вона має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію. За ст. 155 Господарського Кодексу комерційна таємниця належить до об'єктів прав інтелектуальної власності у сфері господарювання. В Кодексі не тільки дано визначення поняття "комерційна таємниця", але й зазначено, що до неї можуть бути віднесені відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть вважатися комерційною таємницею. Між тим, досягти конкретики з найважливіших питань захисту комерційної таємниці в одному нормативному акті неможливо. Право не тільки в загальній формі проголошує необхідність захисту комерційної таємниці, але й містить конкретні норми, що забезпечують його реалізацію.

Слід відзначити, в комерційне право входять лише ті норми, що безпосередньо чи опосередковано стосуються здійснення підприємницької діяльності. Кримінальне законодавство України містить ряд норм, здатних певною мірою забезпечити захист комерційної таємниці [57]. Захист комерційної таємниці кримінальним законодавством здійснюється передусім нормами, об'єднаними в спеціальний розділ Особливої частини Кримінального Кодексу України: "Злочини в сфері господарської діяльності" (ст. 231 — Незаконне збирання з метою використання або використання відомостей, що становлять комерційну таємницю; ст. 232 — Розголошення комерційної таємниці).

Зупинимося на визначенні відомостей, які не можуть становити комерційну таємницю. Постановою Кабінету Міністрів України від 09.08.93 р. № 611 "Про перелік відомостей, що не становлять комерційної таємниці", встановлено, що комерційну таємницю не становлять: установчі документи; документи, що дозволяють займатися підприємницькою, господарською діяльністю чи її окремими видами; інформація у всіх встановлених

формах державної звітності; дані, необхідні для нарахування і сплати податків та інших обов'язкових платежів; документи про сплату податків та обов'язкових платежів; документи про платоспроможність; відомості про участь посадових осіб підприємств в кооперативах, малих підприємствах, союзах, об'єднаннях та інших організаціях, що займаються підприємницькою діяльністю; відомості, що у відповідності з діючим законодавством підлягають оголошенню. Ці відомості підприємства зобов'язані надати органам державної виконавчої влади, контролюючим та правоохоронним органам України, а також іншим юридичним особам на їх вимогу [9].

Таким чином, до переліку відкритих відомостей віднесені документи, що стосуються майже всіх напрямів підприємницької діяльності як у сфері виробництва, так і в сфері послуг.

У ст. 62 Господарського Кодексу України визначається: "Підприємство — самостійний господарюючий статутний суб'єкт, створений компетентним органом державної влади або органом місцевого самоврядування, або іншими суб'єктами для задоволення суспільних та особистих потреб шляхом систематичного здійснення виробничої, науково-дослідної і комерційної діяльності в порядку, передбаченому законодавством" [2]. Отже, керуючись цим визначенням, до числа підприємств можна віднести і комерційні банки. Відомості про операції, рахунки та вклади клієнтів, а також про кореспондентів банків становлять банківську таємницю, що випливає із редакції ст. 52 Закону України від 20.03.91 р. "Про банки і банківську діяльність".

А згідно з постановою Кабміну "Про перелік відомостей, що не становлять комерційної таємниці" банки зобов'язані без пред'явлення їм письмового обґрунтування видавати інформацію, що стосується операцій, рахунків своїх клієнтів, державним податковим інспекціям, а слідчим органам — ще на стадії попереднього слідства [9].

Згідно зі ст. 30 Закону України "Про інформацію" інформація з обмеженим допуском, виходячи із правового режиму, поділяється на конфіденційну та секретну. До конфіденційної інформації відносяться відомості, що знаходяться у володінні, користуванні чи розпорядженні окремих фізичних чи юридичних осіб і розповсюджуються за їх бажанням відповідно до передбачених ними умов.

Перейдемо тепер до розгляду тих вихідних позицій, що є визначальними в дослідженні проблеми правового захисту комерційної таємниці. В першу чергу слід проаналізувати ст. 30 Закону України "Про інформацію". Виходячи із її редакції, правовий режим допуску до відповідної інформації комерційного і банківського характеру, включаючи належність її до категорії конфіденційної, визначають самостійно громадяни, юридичні особи, що володіють такими відомостями. Разом з тим серед цієї інформації є й така, правовий режим якої вже встановлений Верховною Радою України за поданням Кабінету Міністрів України (наприклад, з питань статистики, екології, банківських операцій, податків тощо).

Аналіз положень глави 46 Цивільного Кодексу України дає підставу вважати: склад і обсяг відомостей, що становлять комерційну таємницю, порядок їх захисту визначаються керівником підприємства.

Ось чому суперечності в правовому регулюванні режиму комерційної таємниці, зазначені в ст. 30 Закону України "Про інформацію" та главі 46 Цивільного Кодексу України, створюють серйозні труднощі у вирішенні питань ефективності застосування норм права в захисті комерційної таємниці. Все це викликає необхідність детальнішого розгляду деяких правових аспектів, що стосуються надання банками органам внутрішніх справ закритої інформації.

Відповідно до ст. 5 Положення про державну службу по боротьбі з економічною злочинністю, затвердженого Постановою Кабінету Міністрів України від 15.07.93 р. № 510, працівники цієї служби за наявності відомостей про порушення законодавства, що регулює фінансову, господарську та іншу підприємницьку діяльність, мають право:

- "одержувати у встановленому порядку від Національного банку та його установ, комерційних банків та інших кредитних установ необхідні відомості, копії документів, довідки про банківські операції та залишки коштів на рахунках об'єктів, які перевіряються";
- "одержувати безоплатно від підприємств, установ, організацій і громадян інформацію, за винятком випадків, якщо законом встановлений спеціальний порядок її одержання";

- “вилучати необхідні матеріали про кредитні та фінансові операції у встановленому законодавством порядку”.

Розглянемо, що слід розуміти під суперечностями правового регулювання, що виникають при реалізації службою МВС своїх прав в інформаційних відносинах з банками у встановленому законодавством порядку. В Законі України від 20.12.90 р. № 565-XII “Про міліцію” і в Законі України від 20.03.91 р. “Про банки і банківську діяльність” зазначено, що конфіденційна інформація може бути надана тільки за наявності справи і на письмовий запит. Під “справою” власники інформації розуміють кримінальну справу [62].

Для порушення кримінальної справи досить важливе значення мають не тільки відомості, отримані внаслідок вжиття органами внутрішніх справ оперативно-розшукових заходів, а й фактичні дані, одержані із вказаних в законі джерел. Такими джерелами, як відомо, є протоколи слідчих і судових дій, інші документи [5].

У ст. 52 Закону України “Про банки і банківську діяльність” встановлено, що “довідки про операції та рахунки юридичних осіб та інших організацій видаються банками самим організаціям, державним податковим інспекціям з питань оподаткування, а також у випадках, передбачених законодавством; на письмову вимогу судам, органам прокуратури, служби безпеки, внутрішніх справ, Антимонопольного комітету України, державної контрольно-ревізійної служби, господарському суду і аудиторським організаціям. Довідки про рахунки та вклади громадян видаються банками крім самих клієнтів та їх представників, також судам, органам прокуратури, служби безпеки, внутрішніх справ по справах, що знаходяться в їх провадженні”. Про надання державним податковим інспекціям інформації про рахунки та вклади громадян законодавець не згадує [34].

Викладені міркування про сутність суперечностей у деяких нормах права, що не враховують усю інфраструктуру правового регулювання режиму використання банківської і комерційної таємниці, свідчать про необхідність подальшого вдосконалення законодавства в сфері забезпечення захисту конфіденційної інформації.

Законодавчі гарантії права на інформацію — це система правових засобів, встановлених законом для належного забезпечен-

ня права громадян України на інформацію. Закон України від 2.10.92 р. № 2657–XII "Про інформацію" підтверджує інформаційний суверенітет України. Нові форми та принципи соціального мислення: економічного, політичного, правового, морального визначають принципи інформаційних відносин. Термін "принцип" походить від латинського "principium", що означає початок, основа. Основними принципами інформаційних відносин є: гарантія права на інформацію; відкритість, доступність інформації і свобода її обміну; об'єктивність, повнота та точність інформації; законність отримання, використання, розповсюдження та зберігання інформації.

Законодавство про інформацію особливо виділяє гарантії і права на інформацію. В ст. 10 Закону України "Про інформацію" зазначено: "Право на інформацію забезпечується: обов'язком органів державної влади, а також органів місцевого і регіонального самоврядування інформувати про свою діяльність і прийняття рішень; створенням в державних органах спеціальних інформаційних служб чи систем, які забезпечують у встановленому порядку доступ до інформації; створенням механізму реалізації права на інформацію; здійсненням державного контролю за дотриманням законодавства про інформацію; встановленням відповідальності за порушення законодавства про інформацію". Ці положення становлять сутність гарантій на інформацію. Закон проголошує право "вільного доступу суб'єктів інформаційних відносин до статистичних даних, архівних, бібліотечних і музейних фондів; обмеження цього доступу обумовлюється лише специфікою цінностей і особливими умовами їх зберігання, що визначаються законодавством."

Захист прав громадян України на інформацію не обов'язково починається з часу порушення законодавства про інформацію. Будь-яке посягання на права учасників інформаційних відносин важливо попередити. Саме тому закон виконує передусім функцію правової охорони, а не тільки захисту у вузькому розумінні цього слова. Держава, визнаючи право громадян на інформацію, у випадку його порушення зобов'язується забезпечити ефективний засіб правового захисту будь-якій особі. Стан захищеності особи базується передусім на діяльності держави з попередження небезпек, здатних позбавити суспільство фундаментальних матеріальних і духовних цінностей [47]. Способи (методи) охо-

рони прав учасників інформаційних відносин є достатньо різноманітними:

- усунення перешкод, що заважають реалізації права;
- поновлення права, що з будь-якої причини було порушене;
- застосування заходів відповідальності до порушників права.

Закон захищає не тільки право індивіда на інформацію, а й комерційну таємницю, конфіденційну інформацію, що охороняються державою. Серед механізмів захисту прав і законних інтересів громадян від свавілля органів управління і зловживання владою з боку посадовців особливе місце займає інститут омбудсмена. Це є важливий механізм захисту прав людини і зміцнення законності в діяльності органів виконавчої влади. 23 грудня 1997 р. Верховна Рада України прийняла Закон "Про Уповноваженого Верховної Ради України з прав людини". Цей документ закріпив існування в державі посади Уповноваженого з прав людини з метою здійснення парламентського контролю за дотриманням конституційних прав і свобод людини. Метою парламентського контролю, який здійснює Уповноважений, є: захист прав і свобод людини і громадянина, проголошених Конституцією України, законами України і міжнародними договорами України, сприяння правовій інформованості населення і захисту конфіденційної інформації про особу.

У нас особливий інтерес викликає визначення "комерційна таємниця", дане в ч. 2 ст. 505 Цивільного Кодексу України. Там зазначається, що комерційну таємницю можуть мати відомості технічного, виробничого, комерційного, організаційного характеру тощо. Для підприємства нове вирішення виробничого, технологічного завдання може залишатися комерційною таємницею навіть у тому випадку, якщо воно оформлене як раціоналізаторська пропозиція і видане авторське свідоцтво. На винахід може видаватися патент, тобто він набуває спеціальної правової охорони і не потребує такого захисту, як комерційна таємниця. Правовий режим винаходів залежить від форми їх охорони: за допомогою авторського свідоцтва чи за допомогою патенту. Базовим принципом патенту є його відкритість, тобто в офіційному бюлетені здійснюється публікація про винахід, де наводяться його формули, креслення тощо.

З комерційною таємницею пов'язане таке поняття, як інтелектуальна власність. Якщо звернутися до головного у визна-

ченні інтелектуальної власності, то в найзагальнішому вигляді — це інформація, що не відноситься до суспільної, містить цінні, нові комерційні ідеї, які як специфічний товар мають потенційну вартість. Дозволимо собі зауважити, що вартість ідей одноразова.

Всілякі спроби категорично відмежувати поняття "комерційна таємниця" від поняття "інтелектуальна власність" обов'язково призводять до звуження змісту захисту комерційної таємниці та інших відомостей конфіденційного характеру. Активізація науково-дослідних робіт у цьому напрямі дозволить виділити і зрозуміти зміст трьох методів захисту інтелектуальної власності: патент, авторське право і комерційна таємниця.

Вивчення проблеми "правовий захист комерційної таємниці" передбачає розгляд в науковому плані правових, кримінологічних, організаційних, розшукових аспектів цієї діяльності і відноситься до комплексного дослідження, яке відображає закон диференціації та інтеграції знань [16].

Патент (від давньолатинського *patens* — свідоцтво, грамота) на винахід — документ, що видається компетентним органом держави, засвідчує визнання пропозиції винаходом, пріоритет винаходу, авторство та виключне право на винахід. Видача патенту здійснюється відповідно до норм патентного права. Без згоди автора винахід не може бути використано. Тільки він може видавати дозвіл (ліцензію) на використання винаходу чи повністю поступитися патентом.

На рівні нинішнього розвитку правової науки актуальною є відповідь на запитання, яким чином регулюються відносини, що виникають у зв'язку з використанням творів науки, літератури і мистецтва. Норми авторського права містяться, як відомо, в Цивільному Кодексі України. Авторське право поширюється на твори літератури, науки і мистецтва, що мають вираження в об'єктивній формі (рукопис, креслення і т. ін.), саме це дозволяє відтворювати результат творчої діяльності автора. Для охорони авторських прав не потрібно реєстрації чи виконання інших формальностей. Лише стосовно фотографій (і творів, отриманих аналогічним способом) для охорони авторського права необхідним є зазначення на кожному примірнику імені автора, року і місця випуску у світ.

Авторське право складається із ряду правомочностей. Право на авторське ім'я означає, що автору належить вибір способу позначення належності йому твору (справжнє ім'я, псевдонім) і, якщо він від позначення відмовився (анонім), ім'я повинно вказуватися при публікації твору в цілому, цитуванні. Без згоди автора заборонено розкривати псевдонім чи анонім (від anonymos — безіменний, автор листа чи твору, який приховав своє ім'я; твір без позначення імені автора) і вносити зміни в обране ним позначення. Авторське право захищає тільки форму, в якій виражена конкретна ідея, а не саму ідею.

Серед методів забезпечення безпеки комерційної інформації та інтелектуальної власності як її виду відомі патентування і вибір складу, обсягу відомостей, що становлять комерційну таємницю, визначення їх охорони. Характерним для них є захист оригінальної ідеї, її змісту [15].

Слід спеціально зупинитися на деяких питаннях, пов'язаних з використанням (у тому числі неправомірним) знаків для товарів та послуг, а також фірмових найменувань. Відносини, що виникають у зв'язку з набуттям і реалізацією правоздатності на знаки для товарів та послуг регулюються Законом України від 15.12.93 р. № 3689-XII "Про охорону прав на знаки для товарів і послуг". Порядок використання фірмового найменування регулюється спеціальним нормативним актом, яким є Положення про фірму, затверджене постановою ЦВК і РНК від 22 червня 1927 р.

Товарний знак — позначення, що вміщується на товарі (чи упаковці) промисловими і торговими підприємствами для індивідуалізації товару і його виробника (продавця). Товарні знаки можуть бути вербальними (сукупність окремих літер, цифр, прізвище), образотворчими (малюнки, географічні символи, сукупність кольорів), об'ємними (форма виробів чи упаковка), комбінованими тощо.

Товарний знак виконує функції гарантії якості товару та його реклами. Його застосовують у внутрішній і міжнародній торгівлі. Порядок набуття права на торговий знак, його використання та захист визначається законодавством України і міжнародними угодами.

Подавши до Державного патентного відомства України заявку на реєстрацію знака для товарів та послуг, юридична особа

при позитивному вирішенні питання отримує відповідне свідоцтво, що гарантує правову охорону товарному знакові. У випадку неправомірного використання фірмового найменування, товарного знака без згоди власника від місцевого відділу Антимонопольного комітету України порушник отримує припис припинити такі дії. У випадку реєстрації Міжнародним бюро Всесвітньої організації інтелектуальної власності знака для товарів та послуг, що відповідають рівню міжнародної класифікації, вказується строк дії міжнародної реєстрації.

Предметом злочину, передбаченого ст. 229 КК України (незаконне використання товарного знака), можуть бути:

а) чужий знак, тобто спеціальне позначення для товарів та послуг, на яке власник має свідоцтво Держпатенту;

б) фірмове маркування товарів.

Незаконне використання чужого товарного знака здійснюється умисно з метою отримання прибутку.

2.2. Характеристика суб'єктів і об'єктів охорони комерційної таємниці

Як ст. 231 КК України про відповідальність за підприємницьке шпигунство, так і ст. 232 КК України про відповідальність за розголошення комерційної таємниці спрямовані на захист підприємців. Предметом посягання при розголошенні комерційної таємниці, підприємницькому шпигунстві можуть бути тільки відомості, що мають комерційну таємницю. Кримінальній відповідальності за незаконне розголошення комерційної таємниці підлягають лише спеціальні суб'єкти, тобто особи, яким відомості, що мають комерційну таємницю, стали відомі у зв'язку з їх професійною чи службовою діяльністю і які юридично зобов'язані зберігати ці відомості. Такими суб'єктами можуть бути визнані співробітники податкових інспекцій, банків, правоохоронних органів та інші особи, які відповідно до законодавства мають право знайомитися з відомостями, що становлять комерційну таємницю, чи мають доступ до таких відомостей за службою [52]. В Законі України від 25.03.92 р. № 2229-XII "Про Службу безпеки України" зазначено: "...не підлягають розголошенню відомості, які містять державну, службову і комерційну

таємницю, а також інформація конфіденційного характеру, розголошення якої може завдати шкоди національній безпеці України, честі і гідності особи або порушити її законні права…" [48].

Законом України від 4.12.90 р. "Про державну податкову службу в Україні" в редакції від 24 грудня 1993 р. на працівників податкових інспекцій покладено обов'язок зберігати комерційну і службову таємницю [6].

З об'єктивної сторони, такий злочин, як розголошення комерційної таємниці, охоплює діяння, вчинені умисно громадянами України, іноземцями, особами без громадянства, і полягає в порушенні умов розповсюдження такої інформації (без згоди її власника).

Підприємницьке шпигунство є злочином умисним. Умисел може бути прямий і побічний.

Оскільки захист комерційної таємниці спрямований на забезпечення економічних інтересів підприємства, відповідно, економічна та інформаційна безпека підприємства тісно взаємопов'язані [27].

Українське законодавство зміцнило свої позиції з питань захисту інформації з обмеженим доступом у зв'язку з прийняттям ряду законів, наприклад "Про банки і банківську діяльність", "Про державну таємницю", "Про інформацію", "Про науково-технічну інформацію" [50]. З урахуванням чинних норм кримінального, цивільного, трудового та інших галузей права виявилася можливість проаналізувати вже сформовану в Україні нормативну базу, що лежить в основі захисту комерційної таємниці.

Розгляд в цілому інформації з обмеженим доступом дозволяє виділити в складі всього масиву два самостійні підрозділи, що включають: а) інформацію, що відноситься до державної таємниці; б) інформацію, що має таємницю і перебуває у власності окремих фізичних чи юридичних осіб.

Згідно зі ст. 30 Закону України "Про інформацію" до інформації з обмеженим доступом відноситься:

- конфіденційна інформація;
- інформація, що містить комерційну таємницю;
- інформація, що становить банківську таємницю.

За своїм правовим режимом конфіденційна інформація відноситься до інформації з обмеженим доступом. Конфіденційний

[лат. confidentia — довіра] — не підлягає розголошенню, секретний. Конфіденційна інформація — це "... відомості, які знаходяться у власності, користуванні чи розпорядженні окремих фізичних чи юридичних осіб і розголошуються за їх бажанням у відповідності до передбачених ними умов" [62, *27*].

Тепер про банківську таємницю [37]. Керуючись ст. 52 Закону України від 29.03.91 р. "Про банки і банківську діяльність", банківську таємницю становлять відомості про операції, рахунки і вклади клієнтів, а також про кореспондентів банків [86].

Щодо суб'єктів прав власності на комерційну таємницю Г. К. Нікіфоров, проаналізувавши чинне законодавство України, пише: "Суб'єктом права власності на комерційну таємницю є: держава, громадяни України, інших держав, підприємства, установи, організації всіх форм власності, які здійснюють свою діяльність відповідно до законодавства України і визначили інформацію, яка становить їх комерційну таємницю, або придбали її у встановленому законодавством порядку як комерційну таємницю" [62, *31*].

Що ж стосується права власності на інформацію, що має комерційну таємницю, то його регулююча, охоронна роль на сьогодні очевидна. Порушення права власності на комерційну таємницю може завдати її власнику економічних втрат [38].

Ми вважаємо, до числа об'єктів права власності на інформацію, що становить комерційну таємницю, слід віднести: джерела інформації, що належать власникам комерційної таємниці; ідеї, комерційні інтереси; звіти про ділові переговори; програмні продукти, технічні проекти; нове конструктивне рішення, пристосування, що відносяться до раціоналізаторських пропозицій, "ноу-хау"; структура ціни, відомості про інвестиції; маркетингові дослідження; зміст контрактів, договорів; калькуляція виробничих витрат, плани розвитку підприємства; результати засідань органів управління підприємством тощо [36].

Нині в Україні розроблені основні концептуальні положення правового захисту комерційної таємниці, що повинні втілюватись у практику при створенні на конкретному підприємстві відповідної системи захисту комерційної таємниці і режиму доступу до неї [59]. Концепція [лат. conceptio — сприйняття] — це система поглядів на ті чи інші явища (Краткий словарь иност-

ранных слов. — Государственное издательство иностранных и национальных словарей. — М., 1950).

Зміст ринкових відносин передбачає конкуренцію між суб'єктами фінансово-господарської діяльності [32]. Ця обставина зумовила необхідність виділення на законодавчому рівні інформації, якою володіють суб'єкти приватнопідприємницької сфери діяльності і яка містить комерційну таємницю. Закріплення права підприємства на комерційну таємницю дозволяє йому при створенні системи захисту комерційних секретів втілювати обов'язкові концептуальні положення і принципи, що стосуються зазначеного аспекту безпеки підприємництва [18].

Проблема здійснення ефективних заходів, спрямованих на збереження своїх комерційних секретів, має дві сторони: практичну, коли йдеться про діяльність, спрямовану на створення чи використання системи захисту комерційної таємниці підприємства; і теоретичну, тобто дослідження наукою завдань реалізації права власності підприємств і підприємців на цю категорію інформації з обмеженим доступом [50].

Предметна сфера захисту інформації як комерційної таємниці, що створюється на підставі концептуальних положень і принципів, які визначають також і зміст процесів забезпечення інформаційної безпеки, ось те "головне", що безпосередньо використовується практикою. В сфері захисту інформації багато зусиль доклав спеціаліст із США А. Патокоса, яким була запропонована концепція системного підходу до захисту конфіденційної інформації. Г. К. Нікіфоров пише: "Сутність методу полягає в тому, щоб припиняти, попереджувати чи обмежувати відтік тієї частини інформації, яка може надати конкуренту можливість дізнатися, передбачити, що робить чи планує фірма, і в результаті випередити її на ринку" [62, *16*]. Логіка міркування тут є такою: проблема безпеки, в тому числі й інформаційної, передбачає відсутність, попередження, обмеження чи зняття небезпек і загроз. Образно висловлюючись, людина як істота розумна має можливість попереджувально боротися за збереження безпеки. У зв'язку з цим не можна, звичайно, не погодитись із запропонованою А. Патокосом концепцією системного підходу до забезпечення захисту комерційних секретів, яка отримала назву методу "opsec" (operation security). Системний розгляд ор-

ганізації захисту інформації за методом “opsec” складається із семи етапів:

- аналіз об’єкта захисту, спрямований на визначення, що слід захищати;
- виявлення загроз для фірми;
- аналіз ефективності діючих підсистем забезпечення безпеки фірми;
- визначення необхідних методів і засобів забезпечення безпеки фірми, збереження конфіденційної інформації;
- розгляд і оцінка керівниками фірми пропозицій, поданих службою безпеки і спрямованих на реалізацію додаткових заходів щодо збереження комерційних секретів і їх ефективності;
- практична реалізація додаткових заходів стосовно забезпечення економічної безпеки фірми з врахуванням її пріоритетів і визначення доцільної послідовності здійснення конкретних заходів;
- контроль та інформування персоналу фірми про реалізацію додаткових заходів безпеки.

Ознайомлення з документами та іншими носіями інформації, що класифіковані як комерційна таємниця підприємства, здійснюється з урахуванням умов режиму, встановленого керівником (власником) підприємства. За правовою природою режим — це урегульовані підзаконними нормативними актами (наказами, інструкціями) спеціальні: а) правила допуску працівників підприємства до закритої інформації і б) дії адміністрації щодо забезпечення умов її збереження, а також використання персоналом відомостей, що становлять комерційну таємницю підприємства.

Оскільки йдеться про режим, то доцільно підкреслити, що з його допомогою встановлюються відповідні вимоги і правила використання інформації, яка містить комерційну таємницю, і забезпечення її збереження.

При створенні надійного механізму захисту комерційної таємниці підприємства слід враховувати, що методи, які застосовуються для цього, повинні бути правомірними. Аналіз практики, що склалася в Україні в сфері захисту комерційних і державних секретів, дозволяє зробити висновок, що ці два види діяльності мають багато спільного. Зокрема, ефективну діяль-

ність із захисту конфіденційної інформації в інтересах власника неможливо собі уявити без організації роботи щодо допуску співробітників підприємства до комерційної таємниці. У зв'язку з цим потрібно не тільки враховувати, а й використовувати ті прийнятні вимоги, що характерні для порядку допуску громадян України до державних секретів. Однак під час аналізу його сутності об'єктивно виникає питання про те, що розуміється під терміном "допуск до комерційної таємниці". На нашу думку, існують істотні підстави розглядати це поняття в його практичному і теоретичному розумінні. Практична сторона — це певні організаційні дії адміністрації підприємства щодо оформлення прав співробітників на допуск до комерційної таємниці. Теоретична сторона пов'язана з вирішенням питань: про можливість скоєння працівником, який отримав допуск до комерційної таємниці, тих чи інших дій стосовно закритої інформації; виникнення юридичних обов'язків і наслідків, які можуть мати місце у випадках, коли порушуються вимоги щодо збереження довіреної працівникові комерційної таємниці підприємства.

Звернімось до Закону України "Про державну таємницю", в якому термін "допуск до державної таємниці" визначений як "оформлення права громадянина на допуск до секретної інформації". Як зазначає Г. К. Нікіфоров, "допуск до комерційної таємниці" — це "письмове розпорядження керівника (власника) підприємства чи уповноваженої ним особи, що надає конкретному співробітнику підприємства право на роботу чи ознайомлення з документами, виробами та іншими носіями інформації, які класифіковані підприємством як комерційна таємниця" [62, *50*].

Ступінь важливості відомостей, що знаходяться у володінні, користуванні чи розпорядженні фізичних або юридичних осіб, визначається, передусім, оцінкою можливих негативних наслідків і розміру збитків у випадку, якщо матиме місце їх відтік. На наше переконання, було б помилковим ігнорувати своєчасне включення до найцінніших відомостей тих, що підлягають захисту, не враховуючи існуючий правовий режим інформації комерційного характеру.

В основу визначення конкретного грифу, що обмежує доступ до відомостей, які мають комерційну таємницю, покладено їх

класифікацію з урахуванням такої ознаки, як важливість змісту даних, що використовуються у виробничих та інших цілях.

Усі відомості, що містять комерційну таємницю, можна поділити на три групи:

a) суворо конфіденційні;
b) конфіденційні;
c) не для широкого користування.

Виходячи із оцінки комерційної таємниці, в документ вноситься гриф, що відповідає ступеневі важливості відомостей і обмежує доступ до такого роду інформації, а саме:

a) "комерційна таємниця — суворо конфіденційно" ("кт-ск")
b) "комерційна таємниця — конфіденційно" ("кт-к")
c) "комерційна таємниця — не для широкого користування" ("кт-н/ш. к)

Слід мати на увазі, не можна встановлювати режим обмеженого доступу до загальнодоступної, загальновідомої інформації, що не потребує захисту.

Допуск до комерційної таємниці оформляється відповідно до встановлених ступенів важливості відомостей, з урахуванням виду діяльності, характеру роботи, виконуваної співробітником, його обов'язків, займаної посади тощо.

Правомірність допуску до комерційної таємниці підтверджується в наказі керівника (власника) про дозвіл співробітнику працювати з носіями інформації, що містять комерційну таємницю. Цей акт управління, що видається керівником (власником) підприємства чи уповноваженою ним особою, за юридичною природою є актом застосування норм права, що видається для вирішення конкретного індивідуального питання, пов'язаного з наданням права співробітнику на роботу з відомостями, які мають комерційну таємницю.

Допуск до комерційної таємниці надається дієздатним громадянам України, які досягли 18 років. Позбавляти допуску того чи іншого співробітника до роботи з відомостями, що становлять комерційну таємницю, можуть власник підприємства чи уповноважена ним особа, які раніше таке право працівникові надали. Відповідно до конституційного, цивільного і трудового права особа, чиє право порушене, може в судовому порядку оскаржити рішення керівника підприємства про позбавлення допуску до комерційної таємниці.

З метою вивчення і перевірки кандидата для роботи з відомостями, які мають комерційну таємницю, використовуються методи, передбачені ст. 22 КЗпП України. Для процедур відбору кадрів характерним є витребування співробітниками кадрових підрозділів і служби безпеки документів, що встановлюють особу громадянина, який хоче працювати на підприємстві. Щоб з'ясувати рівень його професійної підготовки, працівники кадрового апарату ознайомлюються з документами про освіту, довідками про стан здоров'я тощо. На практиці вивченню і перевірці кандидата для роботи з відомостями, що становлять комерційну таємницю, притаманні особливості, зокрема складні процеси мислення. Інколи внаслідок некоректних умовиводів у працівників кадрових апаратів складаються помилкові судження, на яких і базуються їхні висновки. На підставі перших, часто помилкових, вражень складається суб'єктивна думка про інтелект кандидата, його психічний стан. Саме ця обставина й спонукає керівників кадрових підрозділів вдаватися до методів психологічної діагностики.

Вивчення і перевірка кандидатур для роботи, пов'язаної з відомостями, що мають комерційну таємницю, спрямовані на досягнення таких цілей:

- виявлення судимостей, злочинних зв'язків, кримінальних нахилів;
- виявлення схильності до скоєння протиправних діянь, необдуманих вчинків під впливом зовнішніх факторів, певних обставин;
- встановлення фактів, що свідчать про морально-психологічну нестійкість під час роботи з носіями інформації, що містять комерційну таємницю.

Одним із поширених методів вивчення особи є метод узагальнення незалежних характеристик, що дозволяє побачити особу з різних сторін. Суттєво доповнює уявлення про особу, яка перевіряється, думка знайомих, характеристики з місць, де вона навчалася, працювала. Оскільки ці відомості є незалежними, вони в цілому дозволяють скласти об'єктивну думку про людину [33].

Для підвищення якості інформації щодо особи, яка перевіряється, першу бесіду з нею доцільно проводити за стандартною формалізованою формою. В подальшому це дозволяє здійс-

нити комп'ютерну обробку відповідей і достатньо швидко отримувати узагальнені відповіді.

Важливо знати, що ознайомчі бесіди (попередня співбесіда) з особами, які приймаються на підприємство, не повинні використовуватися кадровими працівниками для отримання інформації з обмеженим доступом, до якої кандидат мав доступ на попередньому місці роботи. Виконання працівником кадрового підрозділу невластивих даній комунікативній ситуації функцій вступає у протиріччя з рольовими очікуваннями партнера по спілкуванню. В подібних випадках результативнішою може виявитися демонстрація щирого і доброзичливого ставлення до протилежної сторони. Тільки такою поведінкою співрозмовник спонукає до відвертих висловлювань.

Не можна виключити вірогідність провокації з боку кандидата до адміністрації того підприємства, куди він оформлювався на роботу, але не був прийнятий. Бувають спроби скомпрометувати адміністрацію підприємства, що відмовила громадянинові в прийнятті на роботу, скажімо, з залученням засобів масової інформації, коли мусуються твердження нібито мали місце спроби вивідати комерційні таємниці під час оформлення на роботу з вказівкою на підприємство, де це відбувалося.

Для збирання відомостей про кандидатів рекомендується застосовувати такі методи: опитування, анкетування, цільові бесіди з особами за місцем проживання, інтелектуальні психологічні тести, анкетні тести у вигляді опитувальників. Нині спеціалісти (психоаналітики) застосовують стандартизовані психодіагностичні методики, які дозволяють виявити психологічні особливості, властивості характеру, реакції індивіда за різних умов, рівень інтелекту, схильність до швидкої зміни настрою тощо. За результатами тестування можна скласти досить точний психологічний портрет особистості. Частіше інших використовується 16-факторний особистісний опитувальник Р. Б. Кеттела (16-ФЛО).

Службою безпеки при організації роботи з оформлення допуску до комерційної таємниці запрошується психоаналітик. Під час тестування за допомогою 16-ФЛО Кеттела особі, яка випробовується, видається реєстраційний бланк і брошура, що містить 187 питань — стверджень (на практиці їх нерідко заміняє відповідна комп'ютерна програма). На кожне питання може

бути тільки один із трьох запропонованих варіантів відповіді (більшість із них: так — ні, впевнений — ні). "На виході" програма дозволяє отримати графічний профіль особистості обстежуваного і текстовий матеріал з описом характерних особистісних особливостей.

Працівник, на якого оформляється допуск до комерційної таємниці, має взяти зобов'язання про її нерозголошення, а також попередження-зобов'язання про нерозголошення комерційних секретів після звільнення. Зміст цього заходу полягає в тому, щоб створити юридичні гарантії для попередження підприємством можливого відтоку комерційної таємниці до конкурентів через колишнього співробітника, і отримати право на відшкодування цим працівником матеріального чи морального збитку у випадку розголошення конфіденційної інформації. Слід зазначити, що підхід до попередження можливого відтоку комерційної таємниці через колишнього співробітника, відібрання у нього попередження-зобов'язання не суперечить змісту ст. 34 Конституції України і "Положенню про комерційну таємницю підприємства і правила її зберігання".

Всі компоненти організації діяльності щодо збереження від відтоку відомостей про комерційну таємницю перебувають під впливом зовнішнього середовища, а тому мають змінний характер, тобто можуть змінювати свої параметри чи стан у часі. Бажаний результат — збереження комерційної таємниці підприємства багато в чому залежить від умов зовнішнього і внутрішнього середовища. Організаційна система, що забезпечує збереження комерційної таємниці підприємства, тільки тоді ефективна, коли вдається з'єднати її підсистеми (частини) в єдиний механізм. Потреби зовнішнього середовища можуть визначати засоби чи обмежувати діяльність з досягнення організаційною системою своєї мети.

2.3. Розроблення системи захисту інформації з обмеженим доступом, що може бути предметом комерційної таємниці суб'єкта господарювання: технологічний і методичний аспекти

Правове регулювання суспільних відносин у сфері охорони комерційної таємниці передбачає усвідомлення суб'єктами права власності на комерційну таємницю своїх прав і обов'язків, у яких відбивається державна воля у вигляді вимог — обов'язків і дозволів — прав. Механізм правового регулювання правових відносин з питань захисту комерційної таємниці включає такі елементи, як правові норми, правові відносини, правова відповідальність, правова свідомість тощо. Суб'єкти прав власності на комерційну таємницю так чи інакше реагують на вимоги та дозволи, що містяться в нормах права. Розглядаючи даний аспект, не можна не вказати на можливість таких суб'єктів самостійно здійснювати певні дії щодо захисту комерційної таємниці, а також вимагати (у зв'язку з укладеною угодою) певної поведінки від інших осіб, які взяли на себе договірні зобов'язання зберігати в таємниці передані їм відомості.

Слід враховувати, що правовий статус власника комерційної таємниці визначений законом, він характеризує становище суб'єктів права власності на комерційну таємницю стосовно держави, її органів, інших осіб. Доцільно у зв'язку з цим звернутися до визначення поняття суб'єктивне право. Відомо, що це є забезпечена законом міра можливої поведінки громадянина чи організації, спрямованої на досягнення цілей, пов'язаних із задоволенням їх інтересів.

Питання компетенції державних органів, що здійснюють правове регулювання в сфері охорони комерційної таємниці, дедалі частіше входять в орбіту інтересів комерційного права. Уточнимо етимологію слова компетенція [лат. competentia — приналежність згідно з правом] — це коло повноважень певної установи чи особи. У Постанові Верховної Ради України від 16.01.97 р. № 3/97-ВР із змінами, внесеними у відповідності з Законом від 21.12.2000 р. № 217-III "Про концепцію (основи державної політики) національної безпеки України" зазначені основні можливі загрози національній безпеці України в найваж-

ливіших сферах життєдіяльності, серед них і "відтік" інформації, що становить державну чи іншу, передбачену законом, таємницю, а також конфіденційну інформацію, яка є власністю держави [65].

Служба безпеки України відповідно до своїх основних завдань зобов'язана: брати участь у розробці та здійсненні заходів, що стосуються захисту державних таємниць України, сприяти, в порядку передбаченому законодавством, підприємствам, установам, організаціям і підприємцям у збереженні комерційної таємниці, розголошення якої може завдати шкоди життєво важливим інтересам України.

До повноважень СБУ належить подання органам державного управління обов'язкових для розгляду пропозицій, що стосуються питань національної безпеки України, у тому числі призупинення роботи, пов'язаної з державними таємницями, яка здійснюється з порушенням встановлених правил (ст. 25 п. 2 Закону України від 25.03.92 р. № 2229-XII "Про Службу безпеки України").

Право контролю за здійсненням підприємницької діяльності в сфері криптографічного захисту інформації надане Департаменту спеціальних телекомунікаційних систем і захисту інформації СБ України, а також Ліцензійній палаті України (Інструкція про умови і правила провадження підприємницької діяльності (ліцензійні умови), пов'язаної з розробленням, виготовленням, ввезенням, вивезенням, реалізацією та використанням засобів криптографічного захисту інформації, а також з наданням послуг із криптографічного захисту інформації, та контроль за їх дотриманням: Затверджено наказом Ліцензійної палати України та Департаменту спеціальних телекомунікаційних систем і захисту інформації СБУ України від 17.11.98 р. № 104/81).

Згідно з Інструкцією, що регулює умови і правила провадження підприємницької діяльності в сфері криптографічного захисту інформації, суб'єкти, на яких поширюється дія цієї інструкції, зобов'язані:

- допускати співробітників Головного управління криптографічного захисту і розвитку спеціальних телекомунікаційних систем Департаменту, які мають відповідні повноваження, що стосуються контрольних функцій, на свою

територію і забезпечувати їх всією необхідною інформацією;

- невідкладно інформувати Департамент про будь-які обставини, використовуючи які зацікавлені структури (особи) можуть несанкціоновано отримати інформацію про роботи, що мають секретний чи конфіденційний характер.

Окрім криптографічного захисту, підприємницькі структури за дотримання певних умов і правил можуть здійснювати діяльність у сфері технічного захисту інформації [11]. Функції контролю за дотриманням умов і правил провадження відповідних дій щодо технічного захисту інформації покладені на Головне управління технічного захисту інформації цього ж Департаменту СБУ і Управління контрольної роботи Ліцензійної палати.

Необхідно чітко розрізняти такі поняття, як "впровадження системи технічного захисту інформації" і "криптографічний захист інформації". Під впровадженням системи технічного захисту інформації розуміють введення в дію розробленої системи технічного захисту інформації на конкретному об'єкті інформаційної діяльності чи в конкретній інформаційній системі. Доречно наголосити, що забезпечення перевірки достатності рівня захищеності інформації в інформаційній системі шляхом її атестації чи експертизи також входить в перелік функцій з впровадження. Криптографічний захист інформації — це вид захисту, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховання (чи поновлення) змісту інформації, підтвердження її дійсності, цілісності, авторства і т. ін.

Коли йдеться про права і компетенцію учасників правовідносин у сфері комерційної таємниці, то слід виходити з того, що:

- підприємство самостійно визначає комерційні секрети і порядок їх захисту;
- Кабінет Міністрів України визначає відомості, що не можуть становити комерційної таємниці;
- Верховна Рада України створює відповідну законодавчу базу щодо захисту комерційної таємниці.

У відповідності із законодавством підприємство може здійснювати тільки ті види діяльності, що обумовлені в його статуті, тому в ньому доцільно зафіксувати положення про те, що підприємство має право: класифікувати інформацію, що йому на-

лежить, як комерційну таємницю; визначати перелік таких відомостей, їх обсяг, а також порядок захисту і зберігання. Вважається, що саме керівнику чи власнику підприємства, слід приймати рішення про використання відомостей і визначати основні напрями діяльності стосовно захисту таємної інформації. Ця їх компетенція має знайти відбиття у Статуті.

Важливо також зазначити, хто має право вимагати від співробітників виконання встановлених на підприємстві порядку і правил збереження комерційної таємниці (призначається один із заступників керівника підприємства або керівник якого-небудь підрозділу).

Ці положення, зафіксовані в Статуті, дають право:

- вимагати від державних і судових органів захисту інтересів підприємства;
- включати у всі види комерційних договорів вимоги, що стосуються захисту конфіденційної інформації;
- створити власну службу безпеки;
- видавати документи внутрішнього користування з питань забезпечення збереження комерційної таємниці.

Інформація, що становить комерційну таємницю, прирівнюється в правовідносинах до майна і захищається законодавством як право власності на майно і в тому ж порядку. Тому у випадку відтоку інформації підприємство має право вимагати відшкодування економічних втрат, завданих йому конкурентами чи персоналом [64].

У відповідності до постанови Кабінету Міністрів України від 09.06.93 р. № 611 "Про перелік відомостей, які не становлять комерційної таємниці", підприємства зобов'язані надавати ці відомості органам державної виконавчої влади, контролюючим і правоохоронним органам, іншим юридичним особам відповідно до діючого законодавства на їх вимогу [9].

Перейдемо тепер до розгляду деяких актуальних питань теорії, а саме тих, що є визначальними в створенні системи заходів щодо правового захисту комерційної таємниці підприємства. Насамперед слід зупинитися на дозвільній системі доступу співробітників підприємства, органів державної влади і управління, аудиторських структур, українських та закордонних партнерів, клієнтів, контрагентів, конкурентів до інформації, що охороняється. Оскільки система захисту державної і комерційної

таємниці базується на однакових принципах, проте має свої правові особливості, то важливо усвідомити організаційно-правові аспекти роботи, пов'язаної з отриманням дозволу на доступ до комерційної таємниці.

У світлі викладеного необхідно вивчати діяльність тих підприємств, установ, організацій, майно яких не є державною власністю, а управління здійснюється на підставі прав власника щодо господарського використання свого майна і принципів самоврядування трудового колективу.

Законодавством України суб'єктам приватнопідприємницької сфери економіки, що не залучаються до вирішення завдань безпеки держави, дано право встановлювати в інтересах забезпечення збереження комерційної таємниці власні системи заходів стосовно захисту конфіденційної інформації.

Юридичне обґрунтування у законодавстві права підприємства на комерційну таємницю та її захист базується на Конституції України і ряді інших нормативних актів. Зокрема, у Конституції України (прийнятій на п'ятій сесії Верховної Ради України 28 червня 1996 р.) цьому питанню присвячені статті 32, 34, 41, 42, 54; зазначене право базується також на Господарському Кодексі України (16.01.03 р.), на законах України: "Про власність" (07.02.91 р. № 697-XIII), "Про банки і банківську діяльність" (07.12.2000 р. № 2121-XIII), "Про інформацію" (02.10.92 р.), "Про захист від недобросовісної конкуренції" (07.06.96 р. № 236/96-ВР), "Про зовнішньоекономічну діяльність" (16.04.91 р. № 959-XII), "Про науково-технічну інформацію" (25.06.93 р. № 3322-XII), "Про господарські товариства" (19.09.91 р. № 1576-XII), "Про державну таємницю" (21.09.99 р. № 1079-XIV), "Про Службу безпеки України" (25.03.92 р. № 2229-XII), "Про режим іноземного інвестування" (19.03.96 р. № 93/96-ВР), "Про охорону прав на винаходи і корисні моделі" (15.12.93 р. № 3687-XII), "Про охорону прав на промислові зразки" (15.12.93 р. № 3688-XII), "Про страхування" (07.03.96 р. № 85/96-ВР), "Про наукову і науково-технічну діяльність" (01.12.98 р. № 284-XIV), "Про бухгалтерський облік та фінансову звітність в Україні" (16.07.99 р. № 996-XIV), "Про зв'язок" (16.05.95 р. № 160/95-ВР), "Про Національну депозитарну систему та особливості електронного обігу цінних паперів в Україні" (10.12.97 р. № 710/97-ВР) та ін.

Отримання дозволу на доступ до інформації, що охороняється, повинно базуватися на принципі "необхідно знати". Право економічної структури на комерційну, підприємницьку діяльність, на роботу з інформацією, що у відповідності з законодавством України може бути віднесена до категорії "комерційна таємниця", необхідно юридично оформити відповідними документами у встановленому порядку. Тільки після внесення необхідних доповнень в установчі та інші документи, формально надане підприємству право на комерційну таємницю може бути реалізоване практично. Зокрема, повинні бути зафіксовані положення про те, що підприємство має право на комерційну таємницю і організацію її захисту. Як правило, порядок захисту інформації, що містить комерційну таємницю, визначає керівник підприємства. Документами, в які вносять відповідні доповнення, можуть бути: статут, установчий договір, колективний договір, правила внутрішнього трудового розпорядку. А ось Положення про комерційну таємницю і правила її збереження не належить до установчих документів підприємства.

У відповідності з Кодексом Законів про Працю України і Законом України "Про колективні договори та угоди" (01.07.93 р. № 36) колективний договір повинен укладатися між власником підприємства чи уповноваженим ним органом і трудовим колективом незалежно від форм власності і господарювання, які використовують найману працю і мають права юридичної особи. Нині зміст колективних договорів значно розширився, до багатьох з них внесені положення, що стосуються забезпечення збереження комерційної таємниці. Докладно виписано порядок роботи з комерційною інформацією, визначаються взаємні зобов'язання адміністрації і колективу співробітників, встановлено відповідальність за недотримання режиму роботи з комерційною таємницею.

Особлива роль колективного договору в правовому регулюванні правовідносин, що виникають у зв'язку із забезпеченням збереження комерційної таємниці, полягає в тому, що на адміністрацію покладається обов'язок забезпечити навчання працівників, які мають стосунок до конфіденційної інформації підприємства, необхідними інструкціями і методичними матеріалами.

Нормативні положення, у яких встановлюється відповідальність за порушення порядку роботи з комерційною таємницею, повинні розроблятися адміністрацією в межах наданих їй прав, наприклад, притягати порушників до дисциплінарної відповідальності можна тільки в порядку, передбаченому КЗпП України. Крім того, в змісті договору повинно бути передбачено навчання персоналу правилам ведення робіт, пов'язаних з комерційною таємницею.

За своєю сутністю система захисту комерційної таємниці відрізняється від системи захисту державних секретів. При розголошенні державної таємниці матеріальна чи моральна шкода завдається державі. Якщо ж відтік інформації має місце з вини працівника підприємства, то економічна шкода завдається безпосередньо трудовому колективу, і за певних умов підприємство може збанкрутувати [69]. Встановлені у колективному договорі загальні умови роботи персоналу з комерційною таємницею стосуються всього колективу, а не тільки тих працівників, які мають доступ до конфіденційної інформації. Суб'єкти підприємницької діяльності повинні забезпечити режим секретності під час виконання робіт, пов'язаних з державною таємницею. Відповідальність за розголошення державного секрету несе сам працівник, а інколи і його керівник, який недостатньо контролював його діяльність.

Право підприємства, господарського товариства вимагати у судових органів відшкодування персоналом чи конкурентами шкоди і збитків у випадку відтоку з їх вини конфіденційної комерційної інформації виникає тільки за наявності в статуті та установчому договорі юридично визначених підстав і умов.

Підприємства, що створюються і діють на підставі установчого договору і не мають статуту, закріплюють у ньому надане законом право на комерційну таємницю шляхом внесення відповідних нормативних положень. Слід нагадати, що підприємства мають право на добровільних засадах об'єднувати свою виробничу, комерційну діяльність, якщо це не суперечить антимонопольному законодавству України. У відповідності з діючим законодавством договірними об'єднаннями можуть бути асоціації, корпорації, консорціуми, концерни, утворені за галузевим, територіальним та іншими принципами [66]. В об'єднання підприємств, зареєстрованих в Україні, можуть входити підприємства інших держав.

Об'єднання діють на підставі договору чи статуту, що затверджується їх засновниками або власниками. Підприємства України та інших держав, що входять до складу організаційних структур, зберігають за собою права юридичної особи.

Такою ж мірою обґрунтованою слід визнати можливість будь-якого засновника ввійти в об'єднання з власною системою захисту комерційної таємниці. Всі чи ряд засновників мають право спільно здійснювати діяльність, спрямовану на збереження і захист комерційної таємниці. Закон дає засновникам об'єднання право прийняття рішення про спільну власність на комерційну таємницю згідно з установчим договором. При цьому кожен засновник оцінює таку можливість самостійно і з позиції доцільності.

Засновник чи власник підприємства, який має намір закріпити право на комерційну таємницю і забезпечити її захист, повинен мати чітке уявлення про засоби і обмеження, впровадження яких у практику може сприяти попередженню відтоку конфіденційної інформації. Закон дає право юридичній особі вживати заходів, спрямованих на забезпечення збереження комерційної таємниці, що має знайти відображення в правилах внутрішнього трудового розпорядку, які є обов'язковими для виконання не лише персоналом, а й адміністрацією. Адміністрація зобов'язана:

- створити на підприємстві необхідні умови для дотримання персоналом порядку доступу до конфіденційної комерційної інформації і виконання всіма співробітниками встановлених правил забезпечення схоронності інформації з обмеженим доступом до неї (відомості, що становлять комерційну таємницю і ті, що відносяться до конфіденційних);
- проводити роз'яснювальну роботу серед персоналу, формувати у кожного співробітника внутрішнє переконання в необхідності захисту комерційної таємниці і систематично навчати їх тому, як слід запобігати можливому відтоку конфіденційної інформації;
- проводити інструктажі працівників, пов'язаних з доступом до інформації, що віднесена до комерційної таємниці чи є конфіденційною (при зарахуванні в штат, звільненні чи переведенні на іншу посаду);

- вносити в посадові інструкції працівників записи про обов'язки щодо збереження комерційних секретів підприємства і обмеження стосовно виконавців, допущених до комерційної таємниці;
- розробити і реалізувати комплекс організаційних, інженерно-технічних заходів, спрямованих на попередження відтоку конфіденційної комерційної інформації, нейтралізацію загроз безпеки підприємства;
- здійснювати контроль за виконанням працівниками підприємства встановлених вимог щодо збереження комерційної таємниці;
- притягати до дисциплінарної відповідальності працівників за розголошення відомостей, що становлять комерційну таємницю, порушення встановленого порядку поводження з інформацією з обмеженим доступом (відповідно до ст. 147 КЗпП України);
- вживати заходів щодо виявлення і усунення причин і умов, що сприяють вільному доступу персоналу до матеріальних носіїв конфіденційної інформації, відомості в яких значною мірою перевищують необхідний виконавцю мінімум.

Внесення вимог про нерозголошення комерційної таємниці в правила трудового розпорядку є основним організуючим заходом. Цей нормативний внутрішній документ дає право адміністрації вимагати від працівників брати на себе письмові зобов'язання про збереження комерційної таємниці.

Що стосується правовідносин між працівником та адміністрацією, то вони дозволяють: вимагати в судовому порядку від порушника нормативних положень відшкодування господарюючому суб'єкту завданого матеріального чи морального збитку; передавати матеріали в слідчі органи для притягнення до кримінальної відповідальності особи, яка розголосила комерційну таємницю; приймати відповідні рішення на підставі КЗпП України, тобто вдаватися до притягнення винного до дисциплінарної відповідальності, застосовувати санкції у вигляді позбавлення матеріальної винагороди і навіть звільнення співробітника, який втратив довіру.

Не будь-яка інформація може бути віднесена до комерційної таємниці підприємства, оскільки приховування деяких відомос-

тей інколи завдає шкоди суспільству. Загальновідомо, в організації роботи на фондових біржах велике значення має наявність постійної інформації про економічне становище підприємств, зокрема про їхні прибутки чи збитки. Поліпшення економічних показників діяльності підприємства є однією з найважливіших умов, що забезпечують підвищення курсу його акцій на ринку і викликає, як правило, активніший купівельний попит. Треба вказати, що держава має право здійснювати контроль за діяльністю підприємств, у тому числі й податковий. У відповідності з п. 17 ст. 11 Закону України "Про міліцію" органам міліції надане право: "безперешкодно і безоплатно отримувати від підприємств, установ і організацій незалежно від форм власності і об'єднань громадян на письмовий запит відомості, в тому числі і ті, які складають комерційну і банківську таємницю, необхідні в справах про злочини, які знаходяться в провадженні міліції".

Банки видають довідки про операції і рахунки юридичних осіб, інших організацій як самим організаціям, так і державним податковим інспекціям з питань оподаткування, а також на письмову вимогу судам, прокуратурі, Службі безпеки, органам внутрішніх справ тощо у випадках і в порядку, що передбачені Законом України "Про банки і банківську діяльність" (ст. 52) [21].

Комерційна таємниця не потребує державної реєстрації. Однак відомості, що захищаються, дають переваги у конкурентній боротьбі [13]. Важко переоцінити, наприклад, значення судового захисту комерційної таємниці. Вважається, що зараз найпоширенішим правовим способом захисту комерційної таємниці є пред'явлення позову відповідачеві про відшкодування збитків, завданих розголошенням конфіденційної інформації. Можуть бути подані й інші позови залежно від конкретних обставин справи. Перелік відомостей, які не можуть становити комерційну таємницю, визначив Кабінет Міністрів України у своїй Постанові від 09.08.93 р. № 611 "Про перелік відомостей, які не є комерційною таємницею", що дозволило встановити умовні межі можливого віднесення інформації до комерційної таємниці.

Доречно зазначити, що дія цього підзаконного нормативного акта поширюється тільки на відносини, що виникають у сфері розмежування відомостей, що мають комерційну таємницю, і загальнодоступної інформації, що не потребує захисту. Юридич-

не закріплення за підприємством права класифікувати належну йому інформацію як комерційну таємницю, визначати її склад і порядок захисту спрямоване передусім на досягнення кінцевої мети — отримання прибутку. Тому, організовуючи захист інформації, що належить підприємству на правах комерційної таємниці, доцільно приділяти велику увагу тим відомостям, що мають першочерговий інтерес для конкурентів. До їх числа можна віднести інформацію, що стосується технологічних аспектів підвищення конкурентоспроможності товарів за ринкових умов [22].

Оголошуючи ті чи інші відомості комерційною таємницею, важливо пам'ятати — ринок потребує рекламування продукції, що виробляється, та послуг. Аналіз практики свідчить, нині не виключена можливість надмірного засекречення інформації. Тому доцільно виділити ту інформацію, яку можна було б використовувати як рекламу з метою прямого чи опосередкованого отримання прибутку, розширення ринку збуту товарів, що виробляються, та послуг.

Раціоналізаторська пропозиція щодо вирішення технології виробництва може залишатися комерційною таємницею підприємства навіть після отримання авторського свідоцтва. А, скажімо, запатентований винахід не потребує захисту як комерційна таємниця, оскільки має спеціальний правовий захист. Доцільно підкреслити, що патент є способом захисту промислової, а не комерційної інформації.

Вирішення проблеми виокремлення із підприємницької інформації відомостей, що підлягають захисту від конкурентів і комерційного шпигунства, має свої особливості. Так, перш ніж віднести ті чи інші відомості до особливо корисних, необхідно визначити їх справжню чи потенційну цінність для підприємця. Насамперед підприємця повинні цікавити такі властивості інформації, як достовірність, повнота і своєчасність відомостей, власником яких він є, оскільки саме вони створюють вигідні умови для прийняття відповідного рішення і багато в чому визначають його змістовну сторону. Такий підхід забезпечує власнику підприємницької інформації точніше визначення цінності для своєї господарської діяльності відомостей, що розглядаються ним як засіб досягнення позитивного результату (прибутку). Предметний аналіз підприємницької інформації з позиції цін-

ності для її власника дозволяє виділити окремі групи відомостей, що підлягають захисту, оскільки вони містять комерційну таємницю.

Важливе значення має правильна організація роботи за методикою визначення відомостей, що можуть бути віднесені до комерційної таємниці. Хоча вона й узагальнена, допускає різні варіації залежно від особливостей діяльності підприємства, а також внутрішніх і зовнішніх умов. Насамперед зупинимося на умовах, що необхідні для успішного виділення спеціалістами експертної групи кола відомостей, що становлять комерційну таємницю, а також їх ранжирування за категоріями важливості залежно від цінності для підприємства і можливого розміру збитку у випадку розголошення.

Наказом керівника підприємства створюється комісія (у складі 4–5 осіб) для розробки "Переліку відомостей, що становлять комерційну таємницю". До її складу доцільно включити одного із заступників керівника підприємства, який має повне уявлення про функціональний зміст управління підприємством і його особливості (менеджмент), і провідних спеціалістів основних підрозділів (технологія, право, фінанси), серед них і служби безпеки. Достатньо, щоб у комісії був хоча б один спеціаліст, знайомий з особливостями вирішення окремого питання, що розглядається, а інші мали б загальне уявлення про механізм визначення інформації.

Бажано, щоб до початку роботи члени комісії ознайомилися і були готові дати відповідь на ряд питань:

- визначити види діяльності підприємства, що дають прибуток;
- вивчивши ринок збуту, оцінити, чи перевищує рівень прибутку в певній сфері діяльності показники інших підприємств, на яких виробляється подібна продукція, і чи надаються аналогічні види послуг;
- визначити з найбільшою вірогідністю перспективу рентабельності цих видів діяльності, збереження позицій на ринку і переваг у конкурентній боротьбі.

На першому етапі роботи експертна комісія визначає ті види діяльності, які з економічного і технологічного погляду влаштовують підприємство, і навіть у перспективі даватимуть змогу отримувати прибуток вищий від конкурентів. Це дає підстави вва-

жати, що підприємство володіє комерційною таємницею і експерти мають продовжувати аналіз інформації. Застосувавши такий логічний прийом пізнання, можна визначити спільні ознаки, характерні для відомостей, що віднесені до комерційної таємниці. Вони добре відомі (не бути державною таємницею; відноситись до виробничої діяльності, управління, фінансів, технологічної інформації; мати справжню чи потенційну комерційну цінність і давати переваги над конкурентами; мати обмеження в доступі, які встановлюються на законній підставі керівником підприємства; не підпадати під заборону закону).

Якщо на другому етапі внаслідок аналізу інформації комісія дійде висновку, що вона містить необхідні ознаки, притаманні комерційній таємниці, то експерти переходять до третього етапу експертної оцінки, а саме — чи в пріоритетних сферах діяльності можна досягти конкурентоздатності і прибутковості на ринку продукції та послуг. Переваги у конкурентній боротьбі і прибутковість, як правило, забезпечують нові технології, що дозволяють виробляти продукцію з вищими споживчими якостями і нижчою вартістю; прогресивні зміни в організації виробництва і в управлінні; поліпшені матеріали, з яких вироблено окремі деталі, пристрої, вузли; стратегія маркетингу; зниження собівартості продукції і норм витрати матеріалів і багато іншого.

Характеристики посередницьких технологій, спеціальних прийомів, навичок, послуг, що слугують поліпшенню виробничого процесу, ідеї, які виникають у зв'язку із здійсненням підприємницької діяльності, результати науково-дослідних робіт мають потенційну вартість. Наведений для прикладу далеко не повний перелік компонентів (технічного, економічного, комерційного, соціального характеру) дає змогу підприємству успішно почуватися на ринку. Ці ж компоненти експерти розглядають ще й як фактори, що суттєво впливають на отримання прибутку в певних видах діяльності. Роль підприємства може бути такою:

- забезпечує зайнятість членів суспільства;
- забезпечує доходи власникам майна (акціонерам, державі, приватним особам), а також колективу підприємства;
- забезпечує членам суспільства купівельну спроможність (придбання товарів);
- бере на себе соціальну відповідальність;
- створює прибуток, необхідний для власного розвитку.

Не підлягає сумніву, що успішне виконання підприємством своєї ролі можливе тільки за отримання прибутку. Відомості про фактори, що спрямовані на створення сприятливих умов діяльності і забезпечують прибутковість, підлягають групуванню за класифікуючою ознакою. Вважається доцільним відбирати і групувати не тільки ті фактори, що безпосередньо забезпечують прибутковість, а й численні практичні дії підприємства, органічно пов'язані з одержанням найбільшого доходу (максимізації прибутку). Однак слід пам'ятати, що перший рівень систематизації включає саме ті види діяльності, що безпосередньо дають прибуток.

Далі. Обставини, що мають відношення до потреби підприємства, забезпечують отримання прибутку. Він повинен бути об'єктивно визначений шляхом вивчення інтересів цільового ринку, збалансованості прибутків і купівельного попиту; встановлення видів продукції, що виробляються (реалізуються) підприємством і дають екстраординарні економічні результати чи здатні їх дати, а також ринків споживання, здатних забезпечити екстраординарні результати; концентрації ресурсів і зусиль на тих напрямах діяльності, що можуть забезпечити позитивні кінцеві результати, тощо.

Очевидні відмінності між відомостями про фактори, що безпосередньо забезпечують прибутковість, та інформацією про діяльність, спрямовану на досягнення прибутку, слід враховувати при аналізі відомостей, які необхідно віднести до комерційної таємниці. Такий підхід дозволяє виділити із всієї інформації про діяльність підприємства саме ті відомості комерційного, ділового, виробничого характеру, що потребують захисту. У господарській, підприємницькій, виробничій діяльності використовується умовний "Перелік відомостей, що становлять комерційну таємницю". Так, для відомостей ділового характеру — це, як правило, можуть бути дані про постачальників і клієнтів; інформація про конфіденційні переговори; плани розвитку підприємства і його інвестицій; маркетингові дослідження; відомості про контракти, що плануються; рівень прибутку, структура цін тощо. Для відомостей технологічного характеру — це "ноу-хау", характеристики виробів, що створюються, параметри технологічних процесів, що розробляються; відомості про матеріали, із яких виготовлені окремі деталі; нові

зразки пристроїв, обладнання, що використовуються підприємством, тощо [35]. Для відомостей наукового характеру — це ідеї, винаходи, нові методи організації праці, технічні проекти, програмне забезпечення ЕОМ тощо.

Слід нагадати, що при організації роботи з охорони комерційної таємниці насамперед треба визначити порядок надходження до експертної комісії інформації, необхідної для складання "Переліку відомостей, що становлять комерційну таємницю підприємства". В ході підприємницької, конструкторсько-проектної, науково-дослідної діяльності керівники галузевих підрозділів (автор, виконавець робіт) підприємства прогнозують можливі результати і роблять висновок. Керівник, автор чи виконавець робіт, який підписує контрольну карточку зі стислими висновками, попередньо оцінює інформацію з погляду новизни і можливого віднесення до комерційної таємниці. Експертна комісія отримує контрольну карточку через службу безпеки підприємства, працівник відповідного підрозділу якої в порядку ведення контрольного обліку робить необхідний запис у журналі "Попереднього обліку інформації, що має комерційну перспективу".

Для попередження відтоку інформації і захисту інтересів сторін при укладенні юридичними і фізичними особами договорів до них включаються конкретні положення, спрямовані на забезпечення конфіденційності як самого факту укладення угоди, так і її предмета.

Зовнішньоекономічні угоди торгівельного характеру, пов'язані з поставкою товару і його закупівлею у виробника, а також наданням послуг можуть мати форму контракту купівліпродажу чи торгівлі технічними послугами тощо.

У письмовому договорі з потенційним іноземним партнером, якому надано інформацію про здійснення попередньо узгоджених комерційних операцій щодо угоди, містяться застереження, спрямовані на збереження в таємниці відомостей про предмет і умови майбутнього контракту.

Розглядаючи особливості контракту з іноземними партнерами і зобов'язання сторін щодо збереження конфіденційності щодо його змісту, доцільно внести положення, що забезпечують захист прав контрагента на комерційну таємницю. В розділі "інші умови" слід зробити запис, що цей документ є юридичною

підставою для судового розгляду будь-яких майнових, фінансових і комерційних претензій із зобов'язань сторін. Водночас треба передбачити можливість вирішення спорів між контрагентами у Міжнародному комерційному арбітражі при Торгово-промисловій палаті України. Слід спеціально наголосити, що вибір арбітражу тягне за собою і вибір матеріального права держави за місцем знаходження арбітражу. Норми матеріального права визначають взаємні права й обов'язки учасників господарських, майнових, трудових, сімейних та інших правовідносин.

Матеріальне і процесуальне право можна розглядати як юридичні категорії, що виражають діалектичну єдність двох сторін правового регулювання: безпосередньої юридичної регламентації суспільних відносин і процесуальних форм їх судового захисту.

Права та обов'язки сторін зовнішньоекономічних контрактів визначаються правом країни, вибраної сторонами при підписанні контракту, або досягнутої домовленості між учасниками угоди.

При формулюванні в контракті положень, спрямованих на захист комерційної таємниці, слід керуватися чинними законодавчими і підзаконними нормативними актами, насамперед Законом України "Про зовнішньоекономічну діяльність" від 16.04.91 р. (див. "Відомості Верховної Ради України". — 1991. — № 29. — Ст. 377), яким визначено основи правового і економічного регулювання зовнішньоекономічних зв'язків, а також юридичну відповідальність у цій сфері [55]. Згідно з наказом Міністерства зовнішньоекономічних зв'язків № 75 необхідно в текст контрактів і договорів включати базові умови, що визначають обов'язки сторін щодо вжиття всіх необхідних заходів до захисту комерційної таємниці. Аналогічний правовий припис міститься і в Постанові Кабінету Міністрів України і Національного банку України від 21.07.95 р. № 444 "Про типові платіжні умови зовнішньоекономічних договорів (контрактів) і типові форми захисних застережень до зовнішньоекономічних договорів (контрактів), які передбачають розрахунки в іноземній валюті".

При укладенні зовнішньоекономічних контрактів слід керуватися міжнародними правилами щодо тлумачення комерцій-

них термінів під назвою "Інкотермс" (у редакції 1990 р.). Це належним чином враховано в Указі Президента України від 04.10.94 р. "Про застосування Міжнародних правил інтерпретації комерційних термінів".

В "Інкотермс"-2001 чітко зазначені базові умови контракту і правила, що регулюють операції з його виконання, а також дається тлумачення комерційних термінів.

Предмет попередніх переговорів, що ведуться з потенційними іноземними партнерами до стадії укладення контракту, орієнтовно торкається питань, що стосуються намірів, умов і вимог контрагентів щодо зовнішньоекономічної угоди, яка обговорюється. Серед них можуть бути розглянуті і окремі аспекти, пов'язані з можливістю укладення письмового договору про захист комерційної таємниці майбутнього контрагента. Нині практично не викликає сумніву думка спеціалістів у сфері зовнішньоекономічної інформації про те, що з тактичної точки зору під час попереднього обговорення перспектив майбутньої угоди з іноземними партнерами недоцільно конкретизувати конфіденційні відомості, які підлягають захисту у відповідності з вимогами нормативно-правових актів України [23].

Певний інтерес викликає питання, пов'язане з правовим захистом секретів за зовнішньоекономічними угодами в сфері озброєнь. Треба сказати, що Україна, на відміну від минулих років, обрала шлях укладання міждержавних угод із спеціальних питань, що стосуються захисту секретної інформації і зберігання в таємниці переданих відомостей у зв'язку з укладенням і виконанням контрактів. Тому відомості про подібні угоди не можна передавати третім країнам.

Суб'єктам зовнішньоекономічної діяльності слід приділяти увагу збереженню контрактів, укладених з іноземними партнерами, що містять конфіденційні відомості. Для зберігання документів, у яких у письмовому вигляді викладено зміст контрактів, доцільно використовувати спеціальні вогнестійкі шафи чи сейфи, обладнані сигнальними електронними системами. До речі, контракти слід зберігати окремо від інших конфіденційних документів. Цим має займатися спеціально призначений співробітник. Великі закордонні фірми вводять штатну посаду співробітника, який протидіє викраденню інформації, що становить комерційну таємницю.

При юридичному оформленні тексту підприємницького договору (купівлі-продажу, постачання тощо) слід керуватися тим, що саме в ньому зафіксовано досягнуті угоди двох чи більше сторін, спрямовані на встановлення різноманітних зв'язків між юридичними та фізичними особами. Крім того, враховуються особливості взаємовідносин контрагентів, що виникають у зв'язку з необхідністю збереження комерційної таємниці з різних аспектів угоди. Договір як юридичний факт створює відповідні юридичні гарантії для його учасників, серед них і ті, що стосуються захищеності їх індивідуальних інтересів, орієнтовані на особисту відповідальність кожного за незаконну передачу іншій особі, діловому партнеру конфіденційних відомостей.

У договорі зазвичай закріплюються базові умови, згідно з якими необхідно здійснити ряд обов'язкових дій для попередження можливого розголошення комерційної таємниці. Наголошуємо, що поняття комерційні секрети і виробничі секрети різняться за своєю природою і за структурою. Відомості, що стосуються комерційних секретів, на відміну від виробничих, охоплюють сферу торговельних відносин суб'єкта підприємницької діяльності: організація і розмір обороту, стан ринків збуту, постачальники і споживачі, банківські операції, " ноу-хау", сума і терміни кредитування, перспективи розвитку підприємства тощо.

Охорона комерційних і виробничих секретів суб'єкта підприємницької діяльності зумовлена передусім можливою загрозою економічній безпеці та інтересами конкуренції [25]. Самі ж секрети — це документи, схеми, вироби, до яких немає вільного доступу на законних підставах. За їх розголошення чинним законодавством України встановлена юридична відповідальність. Наприклад, ст. 11 Закону України "Про господарські товариства" зобов'язує учасників господарських товариств не розголошувати комерційну таємницю і конфіденційну інформацію, пов'язану з їх діяльністю.

Як відомо, повсякденна діяльність підприємців насичена проведенням комерційних операцій, попередніх переговорів з потенційними партнерами, укладенням договорів і контрактів, вирішенням питань управління тощо. Під час проведення попередніх ділових переговорів з потенційними партнерами, в ході яких зачіпаються питання, що містять конфіденційні відомості,

доцільно оформляти попереджувальні юридичні документи про те, що кожна із сторін не розголошуватиме комерційних секретів, отриманих в ході переговорів [24]. Документом, що юридично захищає інтереси сторін перемовин, може слугувати "Угода про конфіденційність попередніх переговорів з потенційним партнером".

Наша правова наука ще не має глибоких досліджень, присвячених проблемам підготовки кадрів для роботи з комерційною таємницею, незважаючи на те, що саме кадри справляють вирішальний вплив на організацію діяльності підприємств щодо забезпечення захисту інформації з обмеженим доступом. Нечисленні публікації і наукові праці українських і закордонних авторів не завжди містять конкретні рекомендації з методики навчання персоналу роботі з комерційною таємницею.

У вузах загальноюридичного профілю навчання студентів основам організаторської роботи з відомостями, що мають комерційну таємницю, на нашу думку, повинно стати складовою частиною їх професійної підготовки. Професійна підготовка в сфері організації надійного захисту інформації потребує створення відповідної психологічної атмосфери в колективі, системи відносин, орієнтованої на суворе дотримання всім персоналом основних правил захисту інформації [67]. Виявляється, що впливати на особу, яка порушила правила збереження комерційної таємниці підприємства, значно легше, коли проводиться регулярна робота з формування в колективі самосвідомості, що стосується захисту конфіденційної інформації. В найзагальнішому вигляді ця мета досягається шляхом створення такої атмосфери, коли питання безпеки регулярно ставали б предметом обговорення, відкритих дискусій.

Ключовим моментом у вирішенні проблеми є глибоке усвідомлення керівниками підприємств ролі і місця своїх співробітників у створенні загальної системи захисту комерційної таємниці в усіх структурних підрозділах. При її створенні слід враховувати фактори, що впливають на результативність її функціонування за складних умов недобросовісної конкуренції, підприємницького шпигунства. По-перше, це фактори психологічного характеру: особиста переконаність суб'єкта в необхідності вживати заходи, що ускладнюють протиправні дії конкурента, в можливості досягнення за допомогою відповідних

методів і форм позитивних результатів у забезпеченні збереження відомостей, що містять комерційну таємницю; висока професійна підготовка, сумлінність, дисциплінованість, бажання працювати, сформованість позитивних вольових якостей.

По-друге, це вплив зовнішнього середовища на структури організації, створеної для захисту комерційної таємниці підприємства; забезпечення апаратом управління сприятливих умов для збереження конфіденційної інформації; уявлення про якість інформації, необхідної для успішного вироблення і реалізації управлінських рішень у сфері захисту інформації; досягнення синергізму, тобто одночасного функціонування окремих, але взаємопов'язаних структурних елементів, що забезпечують більш високу загальну ефективність, ніж сумарна ефективність частин, взятих окремо.

При проведенні занять з правового захисту комерційної таємниці підприємства доцільно акцентувати увагу на тому, що до найскладніших завдань в організації ефективного захисту комерційної таємниці слід віднести невизначеність дій конкурентів. Тому служба безпеки повинна концентрувати увагу на виявленні протизаконних дій конкурентів, що створюють реальну небезпеку економічному становищу підприємства. Ці негативні фактори зовнішнього середовища враховуються при аналізі загроз і розробленні ефективної стратегії безпеки підприємства [74].

Ефективність діяльності щодо захисту комерційної таємниці значною мірою залежить від знання причин, що зумовлюють її розголошення, і умов, що сприяють цьому [36]. Англійський лексикограф Семюел Джонсон з цього приводу писав: "Зухвале бажання показати, що тобі довірили таємницю, зазвичай стає головною причиною її розголошення".

Контрольні питання та завдання

1. Розкрийте Ваше власне бачення щодо нормативно-правової основи формування і функціонування системи забезпечення інформаційної безпеки підприємництва.
2. У чому полягають суперечності в законодавстві, що стосуються регулювання взаємовідносин суб'єктів підприємницької діяльності з представниками контролюючих органів,

котрі мають право на отримання у підприємств конфіденційної інформації?

3. Поясніть різницю між правовим режимом охорони комерційної таємниці і захистом прав власності суб'єктів господарювання на комерційну таємницю.
4. Окресліть об'єкти захисту у межах самого процесу правової охорони комерційної таємниці і суб'єктів, які мають вживати заходи в інтересах забезпечення збереження комерційних секретів та іншої важливої інформації.
5. Охарактеризуйте суть організації роботи стосовно створення на підприємстві системи правового захисту комерційної таємниці.
6. Які складові елементи становлять основу системи забезпечення правового захисту комерційної таємниці?

Додаткові завдання

1. Розробити ідеальну модель загрози системі інформаційної безпеки.
2. Розробити власну модель системи інформаційної безпеки.

Розділ III

Методи інформаційного шпигунства та протидія йому

3.1. Перехоплення електромагнітних хвиль, що випромінюються в процесі опрацювання інформації

Захист інформації від відтоку через канали паразитного випромінення проводиться з середини 70-х років. У США була розроблена технологія (SOFT TEMPEST) таємної передачі даних каналами паразитного електромагнітного випромінення за допомогою програмних засобів. У СРСР тоді ж з'явилася спеціальна нормативна документація, що регулює питання захисту інформації, враховуючи й автоматизоване її опрацювання. Це, наприклад, відомі "Норми ПД ІТР" (норми протидії іноземним технічним розвідкам). Деякі вітчизняні ЕОМ випускалися в захисному варіанті (зокрема, ЄС 1845, СМ 1420). Була також розроблена технологія захисту імпортованих персональних комп'ютерів.

Комп'ютер випромінює на всіх частотах, тому перехопивши випромінення, можна отримати корисну інформацію.

Шпигуна насамперед цікавить, з якими документами працюють співробітники і, звісно, її зміст. До цього легко дістатися, якщо зацікавлена особа має доступ до екрана монітора. Вивчення практики захисту інформації у банках свідчить, що досить часто монітори співробітників встановлюють екранами до вікон, а тому використовуючи телеоб'єктиви ("МТО-500" — з відстані не більше 300 м, "МТО-1000" — з відстані не більше 600 м, "ТАИР-3" — з відстані не більше 150 м) можна з сусіднього будинку сфотографувати зображення на екрані монітора. Значний інтерес викликають також роздруківки на *принтерах*.

Більше всього інформації нині зберігається в базах даних та інших файлах, *що розміщені на жорстких дисках серверів*. Доступ до них забезпечує локальна мережа або Інтернет. Найваж-

ливішою інформацією для шпигуна є паролі користувачів, особливо пароль адміністратора локальної мережі. Останнім часом простежуються спроби фізичного проникнення на об'єкти потенційної атаки з метою крадіжки паролів або іншої критичної інформації.

Починаючи з 90-х років минулого століття, паралельно із вдосконаленням ринкових відносин змінювалися форми впливу правопорушників на об'єкти зі стабільним фінансовим становищем:

- початковий етап — психологічні атаки (шантаж, погрози) і фізичні розправами;
- другий етап — недобросовісна конкуренція, неділове партнерство, поява фіктивних фірм, агентів у штаті конкуруючих підприємств і т. д.;
- третій етап — несанкціонований доступ до інформації будь-якими способами, в тому числі й програмними, за рахунок перехоплення паразитного електромагнітного випромінення і наведення (ПЕМВН) в ефірі або за рахунок наведення побічних випромінень на провід електроживлення.

Провода електроживлення і заземлення створюють рамкову антену, тому рівень випромінення комп'ютера збільшується.

Ситуація з забезпеченням безпеки стає ще більш уразливою у зв'язку із всезагальною комп'ютеризацією підприємництва. Корисно нагадати такі аксіоми:

- за забезпечення збереження інформації треба платити, а за відсутність такої — розплачуватися;
- доки не буде вироблено заходів для безпосереднього захисту засобів телекомунікації, в тому числі й засобів обчислювальної техніки (ЗОТ), будь-які інші спроби захистити інформацію марні.

Виникла необхідність розробити технологію захисту інформації, за якої змінні параметри засобів обчислювальної техніки суттєво не впливали б на процес виробництва засобів захисту і виробів у цілому.

Найвідоміші сьогодні перехоплення — це випромінення моніторів. Монітор є "найголоснішим" випромінюючим елементом, оскільки для нормальної роботи електронно-променевої трубки необхідні високі рівні сигналів. Для дешифрування перехопле-

них сигналів монітора не потрібно складного опрацювання. Зображення на екрані монітора і, відповідно, випромінювані ним сигнали багаторазово повторюються. У професійній апаратурі ця обставина використовується для накопичення сигналів і, відповідно, ефективнішої діяльності розвідки.

Професійна апаратура для перехоплення випромінення монітора і відображення інформації коштує десятки тисяч доларів. Якщо розвідувальна апаратура встановлена на невеликій відстані, наприклад, у сусідній квартирі, то для перехоплення випромінення монітора може використовуватися саморобна апаратура, найдорожчим елементом якої є *монітор комп'ютера*, або навіть *дещо доопрацьований побутовий телевізор.*

Перехоплення інформації за рахунок випромінення принтерів, клавіатури обійдеться ще дешевше. Інформація у цих пристроях перехоплюється послідовним кодом, усі параметри якого стандартизовані й широко відомі.

Адміністратори локальної комп'ютерної мережі застосовують усі можливі засоби для розмежування доступу, входять у мережу лише з визначеної станції, коли нікого немає. Однак їм необхідно пам'ятати про радіовипромінення, а непоганий малогабаритний професійний розвідувальний приймач нині коштує лише кілька сотень доларів.

Інформація, що передається в ефір за рахунок випромінення принтерів і клавіатури, — це фактично метод радіорозвідки з використанням прихованого випромінення.

Комп'ютер може випромінювати в ефір не лише ту інформацію, що опрацьовує. Якщо при його збиранні не було вжито спеціальних заходів, то він може слугувати також і джерелом відтоку мовної інформації. Це так званий "мікрофонний ефект", він може здійснюватися навіть через корпус комп'ютера. Під впливом акустичних коливань у корпусі змінюються розміри щілин і інших елементів, через які здійснюється випромінення. Відповідно, випромінення стає модульованим, і все, що ви говорите біля комп'ютера, можна прослухати за допомогою розвідувального приймача. Якщо ж до комп'ютера підключені звукові колонки, то шпигун взагалі може заощадити на встановленні у приміщені, що прослуховується, "жучків".

Таким чином, щоб уникнути відтоку інформації через канали паразитного випромінення, необхідно захищатися [39].

Кабельна система не має активних або нелінійних елементів, тому не може бути джерелом паразитного випромінення. Кабельна система пов'язує між собою усі елементи комп'ютерної мережі. За її допомогою передаються мережеві дані, але водночас вона слугує приймачем усіх наведень і середовищем для перенесення паразитних електромагнітних випромінень. Тому необхідно розрізняти:

- паразитне випромінення, викликане переказуванням через лінію сигналів, називають трафіком локальної мережі;
- прийом і наступне перевипромінення паразитних випромінень від розміщених поруч інших ліній і пристроїв;
- випромінення через кабельну систему паразитних коливань від елементів мережевого активного обладнання і комп'ютерів, до яких під'єднано кабель.

При оцінці захищеності кабельної системи зазвичай цікавляться лише тим, наскільки послаблено паразитне випромінення, викликане сигналами, що передаються через кабель під час мережевого обміну інформацією.

Насправді трафік локальної мережі (локальне випромінення) досить добре захищений від відтоку через канали ПЕМВН. Сучасні кабелі для локальних мереж мають дуже низький рівень випромінення переказаних сигналів. В цих кабелях сигнали переказуються по скрученій парі проводів, причому кількість скруток на одиницю довжини завжди постійна. Завдяки цьому скручена пара досить добре збалансована. В принципі така система взагалі не повинна випромінювати. Наявність екрана у скрученої пари попереджує випромінення кабелем енергії в навколишнє середовище.

Насправді в реальній системі завжди мають місце окремі неоднорідності кабелю. Вони виникають насамперед через некваліфіковане або необережне прокладання кабелю. На поворотах через згинання кабелю змінюється взаємне положення провідників у скрученій парі і, як наслідок, змінюється хвильовий опір. Хвильовим опором називається опір, що його здійснює лінія біжучій хвилі. Хвильовий опір позначається грецькою літерою **Р** (ро) і визначається відношенням напруги до струму в лінії при біжучій синусоїдній хвилі.

$$\mathbf{Р = И\ біж./I\ біж.}$$

Кількість енергії, що надходить на лінію, з плином часу змен-

шується. Енергія, спочатку отримана лінією, продовжує переміщуватися вздовж неї.

Велике значення для впливу на кабель має захисна оболонка.

Якість деелектрика впливає на рівень паразитного випромінення, що виникає в процесі мережевого обміну. На практиці в більшості випадків кабельна система — це відмінна антена для всіх паразитних випромінень обладнання, підключеного до мережі.

Опосередковане випромінення, що виникає в елементах комп'ютера, наводиться на всі проводи кабелю локальної мережі.

Внаслідок цього для паразитних випромінень елементів комп'ютера кабель локальної мережі не можна розглядати як багатожильний провід, що виходить за межі екранованого обсягу.

Процеси, пов'язані з передачею енергії уздовж лінії, однакові. Як відомо, кожен провідник має індуктивність. Тому можна вважати, що кожен провід лінії складається з великої кількості малих "елементарних" індуктивностей. Між проводами виникає ємність, яка тим більша, чим довша лінія. Повна ємність виникає з великої кількості дуже маленьких "елементарних ємностей". Розмірковуючи таким чином, ми робимо висновок, що лінія складається з дуже великої кількості дуже малих індуктивностей і такої ж кількості дуже малих ємностей.

Встановити для цих проводів фільтр, який стримував би паразитне випромінення, неможливо. Тому що паразитне випромінення елементів комп'ютера (жорсткий диск, клавіатура і т. д.) зосереджено у тому самому діапазоні частот, що і спектр імпульсів, які передаються скрученою парою у процесі мережевого обміну.

Застосування екранованої скрученої пари значно поліпшує ситуацію, але не гарантує стримання синфазних (синхронізованих за фазою) наведень. Причин для цього в локальній мережі багато, але головна — заземлення пристроїв, що входять до складу локальної мережі.

За правилами техніки електробезпеки усе активне обладнання локальної мережі повинно мати захисне заземлення, що докорінно змінює здатність кабелів локальної мережі випроміню-

вати синфазно наведені на них коливання, викликані роботою елементів комп'ютера.

Паразитне випромінення елементів комп'ютера наводиться синфазно на провід кабельної системи.

Електричне поле **E**, що створюється наведеним випромінюванням, зосереджується в просторі між жилами кабелю і екранованим плетінням. Зосередження створює умови для обмеження електричного поля [E], яке створене наведеним випромінюванням. Відбувається це так. Наведена напруга призводить до виникнення наведеного струму, який протікає у жилах кабелю **I** пр. і у плетінні кабелю **I** звор.(відн.). При відсутності заземлення магнітне поле, яке викликане проходженням наведеного струму у жилах кабелю, компенсується магнітним полем, яке викликане проходженням наведеного струму, але у зустрічному напрямку, у плетінні кабелю. Тому у незаземленій системі паразитне випромінення елементів комп'ютера, що проникає в екрановані кабелі локальної мережі, може добре обмежуватися.

У разі, якщо все активне обладнання заземлене, випромінення елементів комп'ютера також викликає появу наведеного струму **I** пр. у жилах кабелю. Однак зворотний струм у цьому випадку проходить як у екранованому плетінні кабелю **I** звор., так і в проводах заземлення $\mathbf{I}^1$ звор.

Внаслідок цього у контурі, що створений екранованим плетінням кабелю і проводами (шинами) заземлення, виникає розносний струм. Тому розглядуваний контур для наведеного струму у плетінні кабелю і плетінні заземлення являє собою рамкову антену, інколи дуже великих розмірів.

Саме цей ефект і призводить до того, що при підключені добре захищеного комп'ютера до локальної мережі рівень випромінення комп'ютера (насамперед магнітної складової) значно збільшується незалежно від того, застосовуються екрановані кабелі чи ні.

Необхідно зазначити, що рамкова антена виникає незалежно від того, яким чином і наскільки якісно виконано заземлення. Усунути це явище раціональним вибором системи заземлення неможливо. Єдиний спосіб зменшити випромінення — це підключення захисного заземлення до кожного елемента локальної мережі через фільтр, який має великий опір у широкому діапазоні частот, але малий — на частоті 50 Гц.

3.2. Приховування правопорушником передачі розвідданої інформації, що опрацьовується в комп'ютерній мережі

Методи проникнення у комп'ютерну мережу з метою наступного викрадення інформації різноманітні, найдієвіший — це встановлення в системі програми-закладки.

Програма-закладка, залежно від поставленої мети, може, наприклад, перехоплювати паролі користувачів або за визначеним критерієм знаходити необхідну інформацію на жорстких дисках. Усі системні адміністратори вживають відповідних заходів з попередження спроб відправити електронною поштою зібрану правопорушником інформацію на завчасно обумовлену адресу. Це змусить порушників вигадувати нові методи проникнення до комп'ютерної мережі.

Розвідувальну діяльність правопорушника найбільше ускладнюють два моменти:

- встановити програму-закладку ("троянського коня");
- передати перехоплену інформацію.

На заваді розвідувальної діяльності стоять великі обсяги програми-закладки та даних, що передаються за її допомогою.

Скільки існує людство, стільки існує й проблема обміну інформацією. З однієї сторони, люди прагнуть спілкуватися і обмінюватися інформацією, а з іншої, намагаються приховати від сторонніх як зміст, так і факт її передачі. Тому людство постійно удосконалює засоби перехоплення і приховування. Для приховування інформації застосовують методи криптографії і стеганографії.

Криптографія — це система зміни інформації, щоб вона була зрозумілою лише для посвячених.

Стеганографія — це система зміни інформації з метою приховування самого факту існування таємного повідомлення. Слово ***"стеганографія"*** походить від слів ***"steganos"*** — таємниця і ***"graphy"*** — запис і буквально означає ***"таємний запис"***. Застосування криптографії дозволяє сторонньому спостерігачеві легко встановити факт передачі таємного повідомлення, а стеганографії — приховувати це, більше того, для підвищення рівня захисту таємна інформація може додатково шифруватися.

Методи стеганографії передбачають, що сам факт будь-якого обміну інформацією не приховується, хоча повідомлення обо-

в'язково переглядає цензор. Тому під приховуванням факту існування таємного повідомлення розуміється не лише (можливо, навіть не стільки) те, що цензор не може виявити у повідомлені, яке переглядається, іншого, прихованого повідомлення, а й те, що переказуване повідомлення не повинно викликати у цензора підозри. Тоді канал передачі інформації діятиме і надалі.

Перші згадки про використання стеганографії для захисту інформації датуються ще V ст. до н. е. У Давній Греції, скажімо, таємне повідомлення наносилося на дощечки, які потім покривалися воском, і вони без проблем проходили контроль. Так робив Демерат, як свідчать джерела.

У XV ст. монах Трітеміус (1462–1516 рр.) описав багато різних методів таємної передачі повідомлень. 1499 р. їх записи було об'єднано у книзі "Steganographia". Цей підручник нині можна віднайти в Інтернеті.

Серед прикладів стеганографії можна згадати використання молока або спеціальних симпатичних чорнил для написання таємного послання між рядками звичайного листа.

У Німеччині у роки Другої світової війни для таємної передачі інформації у звичайних листівках і листах застосовували так звані мікрокрапки — маленькі фотокартки, які вклеювалися на місце розділових знаків. У такий спосіб німецькі розвідники, які працювали у США, переправляли у свою країну таємну інформацію, і це не викликало підозрінь у цензури. В одному листі уміщували до 20 мікрокрапок, а кожна з них могла містити не лише текст, а й креслення.

Загальний процес стеганографії виражається формулою:

контейнер + повідомлення, що приховується + стегоключ = стегоконтейнер.

Стегосистема — це сукупність засобів і методів для формування прихованого каналу передачі інформації.

Контейнер — будь-яка інформація, що призначена для приховування таємних повідомлень.

Приховуване (вбудоване) повідомлення — таємне повідомлення, що вбудовується в контейнер.

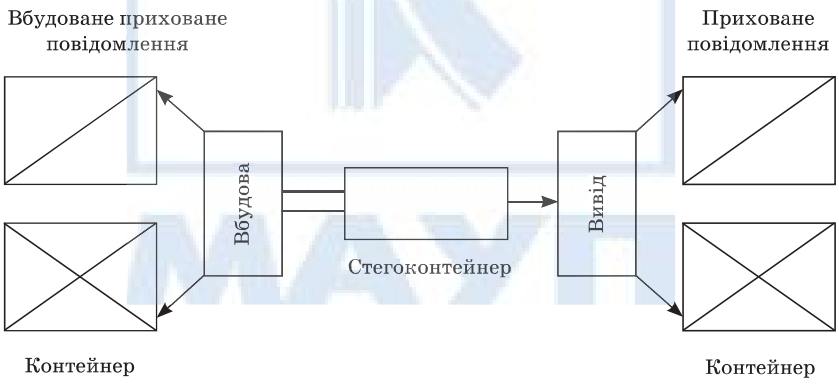
Стегоключ — таємний ключ, необхідний для приховування (шифрування) інформації. Залежно від кількості рівнів захисту (наприклад, встановлення попередньо зашифрованого повідомлення) у стегосистемі може бути один або кілька стегоключів.

Стеганографічний канал (стегокнал) — канал таємної передачі інформації.

Стегоконтейнер — контейнер, що вміщує вбудоване повідомлення.

Для того, щоб сформований за допомогою відповідної сукупності засобів і методів таємний канал передачі інформації був надійним і не викликав підозрінь, необхідно дотримуватися ряд вимог, а саме:

- стегоконтейнер, що вміщує вбудоване повідомлення, для стороннього спостереження практично нічим не повинен відрізнятися від вихідного контейнера;
- при побудові стегосистеми необхідно виходити з того, що "цензор" (системний адміністратор) має повне уявлення про застосовану стеганографічну систему і деталі її реалізації, але невідомою для нього величиною є стегоключ;
- щоб лише власник стегоключа мав можливість встановити факт присутності таємного повідомлення;
- стегосистема повинна бути сконструйована таким чином, щоб лише власник стегоключа мав можливість виділити зі стегоконтейнера вбудоване повідомлення.



Малюнок 1. **Модель стегосистеми**

Комп'ютерна стеганограма — це частина стеганографії, що займається питаннями реалізації стегасистем з використанням комп'ютерної техніки.

Цифрова інформація, як правило, передається у вигляді файлів, тому у комп'ютерній стегосистемі, що являє собою сукупність засобів і методів, які використовуються для формування таємного каналу передачі інформації, використовують поняття *файл-контейнер* і *файл-повідомлення*. Для того, щоб у сторонніх не виникло підозрінь, факт передачі повідомлення (файл-повідомлення) за допомогою стегоключа "змішують" з файл-контейнером. Це не повинно викликати зміни основних властивостей файл-контейнера, що наповнений цифровою інформацією.

Між найпростішим використанням комп'ютерної стегосистеми і симпатичних чорнил багато схожого. Можна білими літерами на стандартному білому тлі редактора Microsoft Word у тексті реклами, скажімо, прального порошку написати кілька рядків таємного послання.

Білі літери на білому тлі не видно, а зробити їх видимими може навіть початківець-користувач персонального комп'ютера. Звісно, надійність такої стегосистеми дуже низька. Проте не дуже складні комп'ютерні стегосистеми уже реально застосовуються зловмисниками, зокрема, "вірусописьменниками".

Відомий, наприклад, вірус під кодовою назвою "W32/Perrun", він "приховує" своє тіло обсягом 18 К у файлі ірj, точніше кажучи, просто додає свій код наприкінці ірj файла. З погляду стеганографії це цілком примітивний метод, проте він дає уявлення про те, як встановити у комп'ютерну систему "програму-закладку" більшого обсягу. Для цього програму-закладку треба зробити двокомпонентною. Стартова частина, яку лише шукає основне тіло програми-закладки в інших файлах, як правило, буває дуже маленькою, що полегшує її встановлення. Однак основна частина програми-закладки може бути за обсягом дуже великою, і при цьому ризик її виявлення можна звести до мінімуму.

Є й складніші механізми маскування. Наприклад, вірус Win 95 CJH встановлюється в "EXE"-файл, використовуючи особливості формату PE (Portable Executable), прийнятого в системі Windows (починаючи з Windows 95). У Windows виконавчий файл "EXE" може утримувати не лише код, а й численні додаткові дані — піктограми, різноманітні службові дані, додаткову інформацію, наприклад, про експортовані й імпортовані функції.

Кожен вид даних, що зберігаються у файлі формату PE, — це окремий об'єкт. Для зберігання всіх об'єктів файл формату PE розбивається на ряд секцій фіксованого розміру. Кожен об'єкт починається з нової секції. Якщо обсяг не займає усього обсягу секції, то ця її частина не використовується і залишається вільною. Тому у файлі формату PE завжди достатньо вільного місця. Найбільше його у першій секції, там записується лише заголовок файлу (PE header). У вільні місця можна сховати чимало інформації, і при цьому ні розмір файлу не зміниться, ні його працездатність не порушиться. Такий механізм маскування дає можливість максимально приховати встановлення у комп'ютері програми-закладки.

Підсумок роботи програми-закладки — знайдені файли.

Можливості сучасних методів комп'ютерної стеганографії можна відчути, провівши експерименти, наприклад, з вільно поширюваними стегопрограмами. Одна з найпоширеніших УТИЛІТ, що здатна приховувати інформацію у графічних (формати gif. bmp) і звукових (формат wav) файлах, — це програма Е. Брауна S — Tools. Вона дає змогу не лише приховати повідомлення, а й зашифрувати його за допомогою стійкого криптоалгоритма, що забезпечить як високу таємність передачі секретного повідомлення, так і його стійкість.

У комп'ютерній стеганографії удосконалюються не лише способи, програми і алгоритми приховування повідомлень, а й пошуки каналів передачі інформації. Дуже зручним каналом для передачі розвіданої інформації є Інтернет, однак не завжди ним можна скористатися, наприклад, через використання міжмережевих екранів чи жорстке адміністрування передачі інформації. Тим паче, що адміністратору системи у пошуках недозволених вкладених файлів, як правило, і непотрібно переглядати кожен файл. Він аналізує адреси, за якими відправляється пошта, і з яких вузлів приймаються файли.

У пошуках нових каналів передачі розвіданої інформації прийшли до ідеї ПЕМВН-вірусів. Давно відомо, що відтік інформації може відбуватися і через канали ПЕМВН. Ці канали незручні лише тим, що некеровані. Щоб отримати потрібну інформацію, треба багато працювати і мати дорогу апаратуру.

Вченим Кембриджа (Андерсену і Куну) прийшла ідея використати як канал для передачі даних паразитні випромінення,

зробивши його керованим. Так було створено технологію SOFT TEMPESS — технологію таємної передачі даних через канали паразитних електромагнітних випромінень за допомогою програмних засобів.

SOFT TEMPESS атака, запропонована Куном, дає можливість за допомогою спеціальної програми-закладки, що проникає з використанням стандартної техніки застосування "вірусів", "червів", "троянців", шукати потрібну інформацію у комп'ютері і передавати її шляхом модулювання зображення монітора. Приймаючи паразитні випромінення монітора, можна виділити корисний сигнал і таким чином отримати таємну інформацію, що зберігається в комп'ютері — паролі, листи, документи.

Ця технологія отримала і другу назву: ПЕМВН-вірус. Вона лише свідчить, що програма-закладка (керує випроміненням комп'ютера, зокрема, монітора) може бути встановлена у цільовий комп'ютер з використанням технології побудови комп'ютерних вірусів. Тому як синонім ми вживатимемо саме цей термін.

Звернімося до механізму маскування передачі розвіданої інформації, що знята з комп'ютера, оскільки це найскладніше в стеганографії. Розвідана інформація передається через випромінення монітора. Для передачі корисного сигналу використовується сигнал монітора. Вивід розвіданої інформації на монітор — це і є спосіб управління випроміненням комп'ютера. Однак при передачі інформації в такий спосіб на екрані виникає характерне зображення ("рябіння"), вид якого визначається частотою амплітудної модуляції. Для управління випроміненням необхідно чітко вибрати той чи інший пристрій серед інших елементів комп'ютера. При цьому програма-закладка реалізується програмно так, щоб формувати спеціальні коди для амплітудної модуляції променя трубки монітора.

Сигнал, що переказується, несе інформацію, яка випромінюється в ефір на визначених частотах. Відбір модуляції оптимізує сигнал для максимально надійного прийому.

Оператор-розвідник використовує відповідну екранну заставку, точніше, зображення, що відіграє роль стегоконтейнера. Таким чином, програма-закладка через визначений пристрій, що є елементом комп'ютера, управляє випроміненням монітора. Модулювати можна не весь екран, а лише необхідну його частину. Характеристики управляючих сигналів підбираються таким чи-

ном, щоб інформація, випромінювана в ефір, відрізнялась від відображеної на екрані.

Зміст способу передачі розвіданих шляхом модуляції зображень монітора базується на тому, що чітко визначеній інформації, відображеній на екрані, відповідають чітко визначені характеристики спектра випромінених одночасно паразитних коливань. Під час передачі монітором зображення, що відіграє роль стегоконтейнера, в ефір випромінюється знайдена програмою-закладкою секретна інформація.

Сигнал передається з монітора за допомогою спеціального АМ-радіоприймача (наприклад AR — 3000A) з його штатною штирьовою антеною і декодованим обладнанням. З'єднувальний кабель пристрою, що управляється паразитним випромінюванням монітора, відіграє роль антени.

3.3. Відповідальність за порушення законодавства про інформацію

Захист прав на комерційну таємницю включає систему заходів, спрямованих на відновлення порушених прав, а також механізм їх реалізації.

Поняття захисту прав у його точному юридичному значенні не слід ототожнювати з поняттям охорони прав, що трактується ширше, оскільки охоплює різні заходи, спрямовані на забезпечення відновлення порушеного права особи. В розглядуваній сфері охороною, а не захистом прав на комерційну таємницю повинні вважатися такі заходи, як, наприклад, страхування ризику розкриття конфіденційної інформації, що має комерційну таємницю, зобов'язання, внесені в договори з працівниками та контрагентами про збереження таємниці, вжиття необхідних організаційних та технічних заходів щодо збереження таємності інформації і т. д. До заходів щодо захисту прав доводиться вдаватися лише тоді, коли права на комерційну таємницю вже порушені або існує реальна загроза їх порушення.

Порушенням прав на комерційну таємницю вважається не будь-яке отримання іншою особою незнайомої їй раніше і цінною для неї в комерційному відношенні інформації, а тільки заволодіння цією інформацією за допомогою незаконних способів.

У такому разі на власника прав на комерційну таємницю покладається обов'язок довести, що конкретна особа отримала доступ до цієї інформації в незаконний, заборонений законом спосіб (наприклад, проникнення в житло, розкриття кореспонденції і т. д.) або всупереч загальним принципам добросовісної конкуренції (підкуп службовців, які не є посадовими особами, отримання інформації від контрагента, власника прав на комерційну таємницю, який зобов'язувався її не розголошувати і т. д.). Якщо довести цього неможливо, то й права особи захисту не підлягають. Захист прав на комерційну таємницю здійснюється практично лише в юридичній формі, тобто у зверненні за допомогою до компетентного органу.

Основною формою захисту прав на комерційну таємницю є юрисдикційна процедура, яка, в свою чергу, поділяється на судову й адміністративну. При цьому переважає судовий порядок захисту прав, який передбачає звернення до суду з позовом про захист порушених прав. Оскільки питання про комерційну таємницю безпосередньо пов'язані з підприємницькою діяльністю, то такі позови загалом відносяться до підвідомчості господарських судів. Якщо відповідачем є працівник, який розголосив комерційну таємницю всупереч трудовому договору (контракту), справа розглядається в суді загальної юрисдикції. Адміністративний порядок захисту прав на комерційну таємницю, він ще називається спеціальним, застосовується лише відповідно до закону (ст. 17 ГК України). Можливість звернення з заявою про порушення прав на комерційну таємницю в Антимонопольний комітет України або його територіальні органи випливає з Закону України "Про захист від недобросовісної конкуренції". У ньому також дається поняття недобросовісної конкуренції, одним із видів якої є неправомірне збирання, розголошення та використання комерційної таємниці.

Загальний, хоч і не повний перелік способів захисту прав на комерційну таємницю наведений у статтях 16 і 434 Цивільного кодексу України. Зрозуміло, не всі вони можуть бути використані, оскільки характер прав та специфіка порушень обмежують варіанти їх вибору. Так, позов про визнання прав на комерційну таємницю може бути розглянуто лише тоді, коли ці права кимось оскаржуються. Наприклад, відповідно до ст. 9 Закону України "Про охорону прав на винаходи і корисні моделі"

роботодавець має право зберігати як комерційну таємницю технологічне або технічне рішення, створене робітником під час виконання службового обов'язку, якщо договором між ними не передбачено інше. Якщо, незважаючи на прийнятий роботодавцем у встановлений законом строк варіант охорони своїх прав, робітник подасть заявку на отримання патенту, роботодавець може захистити свої інтереси, подавши позов до суду про визнання його права на комерційну таємницю.

Аналогічний позов подається й тоді, коли без встановлених законодавством підстав від власника вимагають розкрити конфіденційну таємницю. Такий спосіб захисту прав на комерційну таємницю, як поновлення становища, що існувало до порушення прав, та припинення дій, які порушують право або створюють загрозу його порушення, може бути застосований в тих випадках, коло вчинене порушення ще не призвело до повного припинення прав та є фактична можливість ліквідації його наслідків. Наприклад, особу, яка незаконно заволоділа таємною інформацією, суд може зобов'язати повернути технічну документацію або знищити матеріальні носії, заборонити використання інформації у власних інтересах, а також поширювати її. Власник прав на комерційну таємницю може вимагати визнання недійсним акта центрального органу державної виконавчої влади або органу місцевого самоврядування про розкриття комерційної таємниці, якщо вважає, що дії цього органу виходять за межі його компетенції, в яких нема необхідності, або іншим способом суперечать законодавству. Завдані власнику збитки через порушення прав на комерційну таємницю правопорушник зобов'язаний відшкодувати. Те ж само має зробити і робітник, який розголосив комерційну таємницю всупереч трудовому договору. Це стосується також контрагентів. Збиток повинен бути відшкодований у повному обсязі, тобто компенсації підлягає як реальний збиток, так і упущена вигода. Однак обґрунтувати розмір збитків має сам потерпілий.

Крім цивільно-правових способів захисту прав на комерційну таємницю законодавство встановило і кримінальну відповідальність за посягання на ці права (ст. ст. 231 і 232 КК України).

В останні роки світове співтовариство відкриває для України нові можливості інтегруватися в міжнародну економіку. Важливим фактором формування загальної торгової політики є ство-

рення Світової організації торгівлі (СОТ), що діє на принципах ГАТТ — міжнародно-правової системи, в яку входять також норми і правила створення цивілізованого ринку інтелектуальної власності (угода з торгових аспектів прав інтелектуальної власності (TRIPS)). В р. 7 ч. 2 TRIPS "Охорона інформації, що не підлягає розголошенню", визначені вимоги щодо охорони прав на комерційну таємницю. З метою забезпечення ефективного захисту від недобросовісної конкуренції, згідно зі ст. 10 Паризької конвенції з охорони промислової власності, ГАТТ вперше в історії багатосторонніх договорів розглядає інформацію, що не підлягає розголошенню, як об'єкт інтелектуальної власності. Встановлено критерії, згідно з якими інформація визнається конфіденційною, а також форми її захисту.

З метою приведення національного законодавства у сфері інтелектуальної власності в повну відповідність з нормами угоди TRIPS прийнято Закон України "Про внесення змін до деяких законодавчих актів України з питань інтелектуальної власності". Таким чином, зміни вносяться до Цивільного процесуального, Господарського процесуального, Кримінального, Кримінально-процесуального кодексів України і шести спеціальних законів України: "Про авторське право і суміжні права", "Про охорону прав на винаходи і корисні моделі", "Про охорону прав на промислові зразки", "Про охорону прав на знаки для товарів і послуг", "Про охорону прав на топографії інтегральних мікросистем", "Про охорону прав на зазначення походження товарів" [3].

На наш погляд, навіть у випадку, коли інформація не внесена до переліку відомостей, що не є комерційною таємницею, згідно з Постановою Кабінету Міністрів України № 611, хоча підприємство й нібито правомірно надасть такій інформації статус комерційної таємниці, воно все одно буде зобов'язано її розкрити за вимогою компетентного органу.

Жодне посилання на комерційну таємницю та її захист на рівні закону в цьому випадку не допоможе. Головним аргументом органів влади буде посилання на чинне законодавство України, яким справді ряду органів державної влади встановлено повноваження отримувати інформацію від фізичних та юридичних осіб усіх форм власності, необхідну вказаним органам для реалізації своїх повноважень. Перелік таких органів наводиться в таблиці 1.

Таблиця № 1

№ пор.	Орган, що має право на отримання конфіденційної інформації	Підстава	Відомості і документи, що надаються суб'єктами підприємницької діяльності при перевірці або запиті компетентних органів
1	2	3	4
1.	Служба безпеки України	П. 3 ч. 1 ст. 25 ЗУ "Про Службу безпеки України" від 25.03.1992 р.	Службова документація та звітність з питань державної безпеки України
2.	Орган, що здійснює оперативно-розшукову діяльність	П. 4 ч. 1 ст. 8 ЗУ "Про оперативно розшукову діяльність" від 18.02.1992 р.	Відомості і документи, що характеризують діяльність підприємств, а також спосіб життя окремих осіб, які підозрюються у готуванні або скоєнні злочинів, джерела та розміри їх прибутку
3.	Органи, що ведуть боротьбу з організованою злочинністю	Пп. Б, п. 2 ст. 12 ЗУ "Про організаційно-правові основи боротьби з організованою злочинністю" від 30.06.1996 р.	Інформація, документи про операції, рахунки, вклади фізичних та юридичних осіб. Надається негайно, якщо це неможливо — не пізніше 10 днів
4.	Міліція	П. 17 ч. 1 ст. 11 ЗУ "Про міліцію" від 20.12.1990 р.	Відомості, необхідні у справах про злочини, які знаходяться в проваджені міліції.
5.	Антимонопольний комітет України	Ст. 16 ЗУ "Про Антимонопольний комітет України"від 26.11.1993 р.	Документи та інші відомості, необхідні для проведення перевірки антимонопольного законодавства
6.	Органи дізнання та попереднього слідства	Ст. 66 Кримінального процесуального кодексу України	Документи, які можуть встановити необхідні у справі фактичні дані
7.	Державна комісія з цінних паперів та фондового ринку	Ст. 8 ЗУ "Про державне регулювання ринку цінних	Документи фінансово-господарської діяльності емітентів, осіб, які здійснюють професійну діяльність на ринку

Продовження таблиці 1

1	2	3	4
		паперів на Україні" від 30.10.1996 р.	цінних паперів, фондових біржах та самодіяльних організацій
8.	Органи прокуратури	Ст. 8 ЗУ "Про прокуратуру" від 05.11.1991 р.	Інформація, що необхідна для здійснення прокурорського нагляду або розслідування, видається за вимогою прокурора або слідчого
9.	Державна податкова служба	Ст. 11 ЗУ "Про державну податкову службу в Україні" від 04.12.1990 р.	Грошові документи, бухгалтерські книги, звіти, кошториси, декларації, товарно-касові книги, інші документи, пов'язані з нарахуванням та сплатою податків й інших платежів. Показання РРО та комп'ютерних систем, що використовуються для розрахунків зі споживачами. Наявність свідоцтва про державну реєстрацію, спеціальних дозволів. Пояснення про джерела отримання доходів, нарахування та сплату податків, інших платежів. Інформація про внесення в державний реєстр фізичних осіб — платників податків та інших обов'язкових платежів.

Існує й інший погляд: підприємства не повинні передавати комерційну таємницю будь-яким органам державної влади, крім випадків, коли порушено кримінальну справу і в межах здійснення оперативно-розшукової діяльності.

Контрольні запитання та завдання

1. Назвіть основні способи неправомірного доступу до комп'ютерної інформації з метою перехоплення даних, що знаходяться в комп'ютерній системі або мережі.

ЗАХИСТ ІНФОРМАЦІЇ ТА ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ІНТЕЛЕКТУАЛЬНІЙ ВЛАСНОСТІ

Півень А.Г., *начальник Центру комп'ютерних технологій СумДУ*,
Шевченко І.П., *викладач кафедри АГПФЕБ СумДУ*

Важливим для кожної організації є розробка комплексної програми захисту інформації, що складається з організаційних та програмно-технічних заходів, в якій передбачено розмежування прав доступу, оновлення програмного та технічного забезпечення, навчання персоналу. Абсолютно небезпечну інформаційну систему створити не можливо, тому система безпеки є компромісним рішенням.

Одним з напрямків захисту інформації в інформаційних системах є технічний захист інформації (ТЗІ). У свою чергу, питання ТЗІ розбиваються на два великих класи завдань: захист інформації від несанкціонованого доступу (НСД) і захисту інформації від витоку технічними каналами. Під НСД звичайно мається на увазі доступ до інформації, що порушує встановлену в інформаційній системі політику розмежування доступу. Під технічними каналами розглядаються канали сторонніх електромагнітних випромінювань і наведень (ПЕМІН), акустичні канали, оптичні канали й ін.

Для захисту інформації на рівні прикладного та системного програмного забезпечення використовуються:

- системи розмежування доступу до інформації;
- системи ідентифікації та автентифікації;
- системи аудиту та моніторингу;
- системи антивірусного захисту.

Для захисту інформації на рівні апаратного забезпечення використовуються:

- апаратні ключі ;
- системи сигналізації;
- засоби блокування пристроїв та інтерфейсів вводу-виводу інформації.

В комунікаційних системах (комп'ютерних мережах) використовуються такі засоби мережевого захисту інформації:

- **міжмережеві екрани** (англ. Firewall) **—** для блокування атак з зовнішнього середовища (Cisco PIX Firewall, Symantec Enterprise FirewallTM, Contivity Secure Gateway та Alteon Switched Firewall від компанії Nortel Networks). Вони керують проходженням мережевого трафіку відповідно до правил (англ. policies) захисту. Як правило, міжмережеві екрани встановлюються на вході мережі і розділяють внутрішні (приватні) та зовнішні (загального доступу) мережі;
- **системи виявлення вторгнень** (IDS **—** англ. Intrusion Detection System) **—** для виявлення спроб несанкціонованого доступу як ззовні, так і всередині мережі, захисту від атак типу «відмова в обслуговуванні» (Cisco Secure IDS, Intruder Alert та NetProwler від компанії Symantec). Використовуючи спеціальні механізми, системи виявлення вторгнень здатні попереджувати шкідливі дії, що дозволяє значно знизити час простою внаслідок атаки і витрати на підтримку працездатності мережі;
- **засоби аналізу захищеності —** для аналізу захищеності корпоративної мережі та виявлення можливих каналів реалізації загроз інформації (Symantec Enterprise Security Manager, Symantec NetRecon). Їх застосування дозволяє попередити можливі атаки на корпоративну мережу, оптимізувати витрати на захист інформації та контролювати поточний стан захищеності мережі.

Важливим для підприємства є резервне копіювання важливої інформації та створення копій обрізів системних дисків персональних комп'ютерів та серверів у момент їх нормальної роботи. Поєднання цих заходів дозволять відновити роботу в найкоротший термін.

Обмеження прав на зміну системної інформації, застосуванні автоматизованих правил захисту, планове оновлення та перевірка систем, своєчасний збір та аналіз інформаційної активності під час роботи користувача захистить від випадкових помилок у роботі інформаційної системи. Багато в чому правильні дії в цих напрямках залежать від кваліфікації адміністратора комп'ютерної мережі.

Комп'ютерні віруси, останнім часом, найчастіше проникають в систему через електронну пошту та заражені USB-носії інформації (флеш-карти та ін.).

Сучасний антивірусний захист не може обмежуватись лише встановленням антивірусної програми. Необхідним є застосування спеціалізованих програм одноразової перевірки, які оновлюються щоденно, та контроль автоматизованого запуску з USB-носіїв, наприклад: Dr.Web CureIt!, Kaspersky Virus Removal Tool, Norton Security Scan, Panda USB Vaccine.

Для безпечної роботи в локальній та глобальній інформаційній мережі Інтернет важливим є налаштування параметрів безпеки програми перегляду, а також спостереження за мережевою активністю комп'ютерів мережі з метою своєчасного виявлення та блокування мережевих загроз. Як приклад багатофункційного антивірусного та антишпигунсьго програмного забезпечення для мережі можливо виділити Symantec Endpoint Protection, що включає в себе: програмне забезпечення клієнта, серверну систему підтримки, збору та систематизації інформації, централізоване оновлення та карантин збереження інфікованих файлів.

Для захисту від помилок користувачів під час роботи з важливими документами необхідно застосовувати засоби дозволів до окремих документів та інформації безпосередньо у документі. Це можливо досягнути використовуючи можливості офісних програм: шаблони та захист.

Якщо права на інформаційно-комунікаційну систему підприємства не є його власністю правовідносини визначаються згідно Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» № 80/94-вр. Власник інформаційних ресурсів або уповноважені ним особи мають право здійснювати контроль за виконанням вимог по захисту інформації та забороняти чи призупиняти обробку інформації у випадку невиконання цих вимог, а також може звертатися в органи державної влади для оцінки правильності виконання та дотримання вимог по захисту його інформації в інформаційних системах. Ці органи дотримуються вимог конфіденційності інформації та результатів перевірки.

На підприємствах в даний час широко застосовуються автоматизовані системи АС - системи, що здійснюють автоматизовану обробку даних і до складу яких входять технічні засоби їх обробки (засоби обчислювальної техніки і зв'язку), а також методи і процедури, програмного забезпечення. Захист інформації в АС впроваджується відповідно Закону України «Про захист інформації в автоматизованих системах», що введений в дію Постановою Верховної Ради України № 81/94-ВР від 05.07.94 р. та Закону України "Про електронний цифровий підпис" №852-IV від 22.05.2003.

Важливим фактором інформаційної безпеки є також використання ліцензійного та сертифікованого програмного забезпечення, що дозволяє отримувати своєчасні оновлення захисту та забезпечити стале функціонування та розвиток інформаційної системи підприємства.

Формування ринку інформаційних продуктів та послуг і забезпечення його ефективного функціонування обумовлюється законодавчою підтримкою та правовим захистом. Законодавче врегулювання процесів розвитку інформаційної сфери охоплює цілий комплекс не лише юридичних, а й економічних та технологічних проблем, тому проблема захисту інформації від зовнішніх і внутрішніх загроз в умовах сучасного інформаційного простору, її правове забезпечення є особливо гострою. Ігнорування проблем інформаційної безпеки може призвести до труднощів або й узагалі унеможливити прийняття найважливіших управлінських рішень.

ОРГАНІЗАЦІЯ КОМП'ЮТЕРНОЇ БЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Яроменко І. М.[1], **Орлик О. В.**[2]

1 – студент, кафедра Інформаційних систем в економіці,
2 – канд. екон. наук, доцент, кафедра Інформаційних систем в економіці
Одеський національний економічний університет, м. Одеса

АНОТАЦІЇ

Яроменко І. М., Орлик О. В. ***Організація комп'ютерної безпеки та захисту інформації.*** *Розглянуто деякі питання комп'ютерної та інформаційної безпеки. Проведено аналіз основних захисних засобів персональних комп'ютерів. Охарактеризовано основні технічні складові комп'ютерної безпеки. Визначено актуальні проблеми захисту інформації в інформаційних системах.*
Ключові слова: *комп'ютерна безпека, захист інформації, інформаційні системи, Інтернет.*

Яроменко И. Н., Орлик О. В. Организация компьютерной безопасности и защиты информации. *Рассмотрены некоторые вопросы компьютерной и информационной безопасности. Проведен анализ основных защитных средств персональных компьютеров. Охарактеризованы основные технические составляющие компьютерной безопасности. Определены актуальные проблемы защиты информации в информационных системах.*
Ключевые слова: *компьютерная безопасность, защита информации, информационные системы, интернет.*

Yaromenko I. M, Orlyk O. V. Organization of computer security and protection of information. *Some aspects of computer and information security. The analysis of basic safety equipment of personal computers. Describes the main technical components of computer security. Identified actual problems of information protection in information system.*
Keywords: *computer security, information security, information systems, the Internet.*

ПОСИЛАННЯ НА РЕСУРС

Яроменко, І. М. *Організація комп'ютерної інформації та захисту інформації* / І. М. Яроменко, О. В. Орлик // Інформатика та інформаційні технології : студ. наук. конф., 20 квітня 2015 р. : матер. конф. — Одеса, ОНЕУ. — С. 64-67.

В даний час дуже широко використовується термін «комп'ютерна безпека». За останній час відсоток використання комп'ютерних мереж, а особливо Інтернету значно виріс, тому сьогодні термін «комп'ютерна безпека» використовується для опису проблем, пов'язаних з мережевим використан-

ням комп'ютерів і їх ресурсів. Сучасні інформаційні технології потребують організації високого рівня захисту даних.

Комп'ютерна безпека має велике значення для забезпечення захищення систем обробки та зберігання даних. Об'єктами комп'ютерної безпеки є інформаційні ресурси, канали інформаційного обміну і телекомунікації, механізми забезпечення функціонування телекомунікаційних систем і мереж та інші елементи інформаційної інфраструктури.

Особливості захисту персональних комп'ютерів (ПК) обумовлені специфікою їх використання. Загалом, об'єктом захисту в інформаційній системі є інформація з обмеженим доступом, яка циркулює та зберігається у вигляді даних, команд, повідомлень, що мають певну обмеженість і цінність як для її власника, так і для потенційного порушника технічного захисту інформації. Стандартність архітектурних принципів побудови, обладнання та програмного забезпечення персональних комп'ютерів, висока мобільність програмного забезпечення і ряд інших ознак визначають порівняно легкий доступ професіонала до інформації, що знаходиться в ПК. Для захисту персональних комп'ютерів використовуються різні програмні методи, які значно розширюють можливості по забезпеченню безпеки інформації, що зберігається. Серед стандартних захисних засобів персонального комп'ютера найбільше поширення отримали:

— *засоби захисту обчислювальних ресурсів, що використовують паролльну ідентифікацію і обмежують доступ несанкціонованого користувача;*
— *застосування різних методів шифрування, що не залежать від контексту інформації;*
— *засоби захисту від копіювання комерційних програмних продуктів;*
— *захист від комп'ютерних вірусів і створення архівів.*

Компютерна безпека – це сукупність проблем у галузі зі телекомунікацій та інформатики, пов'язаних з оцінкою і контролюванням ризиків, що виникають при користування комп'ютерними мережами.

Основними технічними складовими комп'ютерної безпеки є:

— ***Конфіденційність (секретність)*** – *означає, що у неавторизованих користувачів не буде доступу до вашої інформації. Наслідки, які можуть бути викликані прогалинами в конфіденційності, можуть варіюватися від незначних до руйнівних;*
— ***Цілісність*** – *означає, що ваша інформація захищена від неавторизованих змін, що не відноситься до авторизованих користувачам. Загрозу цілісності баз даних і ресурсів, як правило, представляє хакерство;*
— ***Аутентифікація*** – *сервіс контролю доступу, який здійснює перевірку реєстраційної інформації користувача. Іншими словами це означає, що користувач – це є насправді той, за кого він себе видає;*
— ***Доступність*** – *означає те, що ресурси доступні тільки авторизованим користувачам.*

Іншими важливими компонентами, яким приділяється велика увага професіоналами в області комп'ютерної безпеки, є контроль над доступом і суворе виконання зобов'язань.

Для користувачів Інтернету найбільш важливою складовою є конфіденційність, тому що більшість користувачів думають, що їм нема чого при-

ховувати або інформація, яку вони надають при реєстрації на сайті, не є секретною. Але потрібно пам'ятати, що в Інтернеті інформація дуже швидко поширюється і потроху зібрана інформація з різних джерел може багато чого сказати про людину. Тому можливість контролю інформації, для чого вона збирається, хто і як може нею скористатися – є дуже серйозним і важливим питанням в контексті комп'ютерної безпеки.

Захист інформації – сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи автоматизованій системі та осіб, які користуються інформацією.

Сьогодні зміст категорії «захист інформації» все більше і більше пов'язується з безпечним функціонуванням автоматизованих (комп'ютерних) систем у всіх галузях суспільної діяльності. Досить актуальна проблема захисту інформації від різних загроз:

— *несанкціонований доступ – 2%;*
— *укорінення вірусів – 3%;*
— *технічні відмови апаратури мережі – 20%;*
— *цілеспрямовані дії персоналу – 20%;*
— *помилки персоналу (недостатній рівень кваліфікації) – 55%.*

Таким чином, однією з потенційних загроз для інформації в інформаційних системах слід вважати цілеспрямовані або випадкові дії персоналу (людський фактор), оскільки вони становлять 75% усіх випадків.

Політика інформаційної безпеки, яку дійсно можна назвати хорошою і ефективною, повинна, перш за все, бути зрозуміла всім користувачам. Для вирішення цієї проблеми рекомендується проводити постійне ознайомлення користувачів з наявною політикою безпеки і не розцінювати такі дії як просту формальність. Користувачі повинні розуміти всю узяту на себе відповідальность і сприяти збереженню інформації.

Широке впровадження комп'ютерів в усі види діяльності, постійне нарощування їх обчислювальної потужності, використання комп'ютерних мереж різного масштабу призвели до того, що загрози втрати конфіденційної інформації в системах обробки даних стали невід'ємною частиною практично будь-якої діяльності.

Інформаційна безпека є складовим компонентом загальної проблеми інформаційного забезпечення людини, держави і суспільства.

ЛІТЕРАТУРА

1. Що таке комп'ютерна безпека [Електронний ресурс] // Портал : arhiv-statey.pp.ua. — Режим доступу \www/ URL: http://arhiv-statey.pp.ua/index.php?newsid=26223. — Заголовок з екрана, доступ вільний, 27.03.2015.
2. Гавловский, В. Інформаційна безпека: захист інформації в автоматизованих системах (організаційно-правовий аспект) [Електронний ресурс] / В. Гавловский // Портал : bezpeka.com. — Режим доступу \www/ URL: http://www.bezpeka.com/ru/lib/spec/law/information-security-automated-systems.html. — Заголовок з екрана, доступ вільний, 27.03.2015.
3 Черкун, О. М. Сучасні технології комп'ютерної безпеки [Текст] / О. М. Черкун // Сучасні технології комп'ютерної безпеки : колективна монографія. — Рівне : МЕГУ, 2012. — 90 с.

4. Безпека банківської діяльності : монографія [Текст] / [Н. Ф. Казакова, В. І. Панфілов, Л. М. Скачек, О. О. Скопа, В. О. Хорошко]. — К. : ПВП «Задруга», 2013. — 282 с.
5. Орлик, О. В. Економічна безпека підприємства: властивості, стратегія та методи забезпечення [Текст] / О. В. Орлик // Економічна безпека в умовах глобалізації світової економіки : [колективна монографія у 2 т.]. — Дніпропетровськ : «ФОП Дробязко С.І.», 2014. — Т. 2. — С. 176-182.
6. Корольов, М. В. Проблематика дослідження питань інформаційної безпеки у державному управлінні [Текст] // М. В. Корольов, О. О. Скопа / Вісник Східноукраїнського національного університету імені Володимира Даля. — Луганськ : СНУ ім. В. Даля. — 2013. — №15(204). — Ч. 1. — С. 88-93.
7. Орлик, О. В. Система загроз економічній безпеці суб'єктів господарювання [Текст] / О. В. Орлик // Вісник соціально-економічних досліджень : зб. наук. праць. — Одеса : ОНЕУ. — 2014. — Вип. 1(52). — С. 250-257.
8. Скопа, А. А. Политика предупреждения угроз информационной безопасности в практической деятельности Одесского филиала ОАО «Укртелеком» [Текст] / А. А. Скопа, Н. Ф. Казакова, С. Т. Сорока // Вісник Національного технічного університету «ХПІ». — Х. : НТУ ХПІ. — 2012. — №17. — С. 42-47.
9. Орлик, О. В. Факторы обеспечения и основные свойства экономической безопасности [Текст] / О. В. Орлик // Modern problems of regional development : Collection of scientific articles. — 2014. — Vol. 2. — P. 190-194.
10. Йона, О. О. Світові тенденції боротьби з кіберзлочинністю [Текст] / О. О. Йона, Н. Ф. Казакова // Вісник Східноукраїнського національного університету імені Володимира Даля. — 2013. — № 15(204). — Ч. 1. — С. 59-62.
11. Орлик, О. В. Финансово-экономическая безопасность предприятия и принципы ее обеспечения [Текст] / О. В. Орлик // Economics and management: theory and practice : collection of scientific articles. — 2014. — Vol. 2. — P. 286-291.
12. Орлик, О. В. Методи управління фінансово-економічною безпекою [Текст] / О. В. Орлик // Сборник научных трудов SWorld. — 2014. — Т. 28. — №. 1. — С. 37-41.
13. Казакова, Н. Ф. Дослідження та застосування в системах захисту інформації кореляційного критерію подібності графічних структур [Текст] / Н. Ф. Казакова, О. О. Фразе-Фразенко // Системи обробки інформації. — 2014. — № 2 (118). — Т 2. — С. 246.
14. Фразе-Фразенко, О. О. Спосіб регуляризації некоректно поставленої задачі розпізнавання у системах телебачення замкнутого контуру [Текст] / О. О. Фразе-Фразенко // Східно-Європейський журнал передових технологій. — 2012. — № 6/4(8). — Спецвипуск (4). — С.19-20.
15. Скопа, О. О. Анізотропна фільтрація зображень у системах аутентифікації [Текст] / О. О. Скопа, О. О. Фразе-Фразенко // Захист інформації і безпека інформаційних систем : II Міжнар. наук.-техн. конф., 30 травня – 01 червня 2013 р. — Львів, НУ «Львівська політехніка». — С. 156-158.
16. Казакова, Н. Ф. Синтез методу виділення контурів у системах ідентифікації на основі усереднення перепадів яскравості [Текст] / Н. Ф. Казакова, О. О. Фразе-Фразенко // Інформаційна безпека. — 2013. — № 2(10). — С. 48-57.