УДК 005.93:005.8:001.891
DOI 10.18372/2786-5495.1.15758

Вівчар Оксана Іванівна
доктор економічних наук, професор,
Західноукраїнський національний університет,
м. Тернопіль, Україна
Шатарський Артур Яремович
радник Міністра молоді та спорту України;
аспірант,
Західноукраїнський національний університет,
м. Тернопіль, Україна

СПЕЦИФІКА ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ: БЕЗПЕКОЗНАВЧІ КОНТЕКСТИ

Анотація. *У статті проведено комплексне дослідження специфіки технічного захисту інформації суб'єкти господарювання з метою забезпечення безпекознавчих умов. На основі чого проведено ідентифікацію складових інформаційної системи на сучасному етапі розвитку.*

Ключові слова: *інформаційна безпека, складові інформаційної системи, технічний захист інформації, технічні каналами, система захисту інформації.*

Annotation. *The article conducts a comprehensive study of specifics the technical protection of information by business entities in order to ensure security conditions. On the basis of which the identification the components of information system at the present stage of development is carried out.*

Keywords: *information security, components of information system, technical protection of information, technical channels, information protection system.*

В сучасних умовах суб'єкти господарювання функціонують у складному, швидкоплинному середовищі, що обумовлює посилення інформаційної безпеки, потреба в забезпеченні високого рівня безпеки, що визначає надзвичайну актуальність дослідження. Експоненціальне зростання кількості злочинів у економічній та інформаційній сферах, стрімке розповсюдження систем електронного документообігу, поява глобальних баз даних (у тому числі – персональної та комерційної інформації) вимагають побудови надійної системи інформаційного захисту суб'єктів господарювання.

Слід відзначити, що технічний захист інформації – це не данина моді, а вимога часу. Адже на сучасному етапі розвитку суспільства інформація є чи не найдорожчим товаром, одним з найважливіших джерел функціонування суб'єктів господарювання. Широкомасштабне впровадження інформаційних технологій потребує значної уваги до питань технічного захисту інформації, оскільки несанкціонований витік її може призвести до втрати суб'єктів господарювання позицій на ринку і значних фінансових збитків [1, с. 430].

Доведено, що одним із напрямів захисту інформації в інформаційних системах є технічний захист інформації. З практичної точки зору варто відзначити, що питання технічного захисту інформації можна ідентифікувати на два великих класи завдань:

– захист інформації від несанкціонованого доступу (НСД);

– захист інформації від витоку технічними каналами.

Наукові дослідження вказують на той факт, що технічні канали – це канали побічних електромагнітних випромінювань і наведень (ПЕМВН), акустичні канали, оптичні та ін. Встановлено, що для розв'язання всього комплексу завдань господарюючий суб'єкт має співпрацювати з провідними підприємницькими структурами, що працюють у галузі захисту інформації, в тому числі зі Службою безпеки України, державним підприємством «Українські спеціальні системи» та ін.

Згідно проведених наукових досліджень варто виокремити, що захист від несанкціонованого доступу може бути здійснений у різних складових інформаційної системи:

− прикладне й системне програмне забезпечення: системи розмежування доступу до інформації; системи ідентифікації та автентифікації; системи аудиту й моніторингу; системи антивірусного захисту;

− апаратна частина серверів та робочих станцій: апаратні ключі; системи сигналізації; засоби блокування пристроїв та інтерфейсів вводу-виводу інформації;

− комунікаційне обладнання і канали зв'язку:

1) міжмережеві екрани (Firewall) – для блокування атак із зовнішнього середовища: Cisco PIX Firewall; Symantec Enterprise Firewall TM; Contivity Secure Gateway та Alteon Switched Firewall від компанії Nortel Networks. Вони керують проходженням мережевого трафіка відповідно до правил (policies) захисту. Міжмережеві екрани зазвичай установлюють на вході мережі і поділяють на внутрішні (приватні) й зовнішні (загального доступу);

2) системи виявлення вторгнень (IDS – 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 Net Prowler від компанії Symantec). Використовуючи спеціальні механізми, системи виявлення вторгнень здатні запобігати шкідливим впливам, що дає змогу значно зменшити час простою внаслідок атаки і витрати на підтримку працездатності мережі;

3) засоби створення віртуальних приватних мереж (VPN – Virtual Private Network) – для організації захищених каналів передавання даних через незахищене середовище: Symantec Enterprise VPN; Cisco IOS VPN; Cisco VPN concentrator. Ці віртуальні приватні мережі забезпечують прозоре для користувача сполучення локальних мереж, зберігаючи при цьому конфіденційність та цілісність інформації шляхом її динамічного шифрування;

4) засоби аналізу захищеності – для аналізу захищеності корпоративної мережі та виявлення можливих каналів реалізації загроз інформації: Symantec Enterprise Security Manager; Symantec Net Recon. Їх застосування дає змогу уникнути можливих атак на корпоративну мережу, оптимізувати витрати на захист інформації та контролювати поточний стан захищеності мережі.

− периметр інформаційної системи, для захисту якого створюються системи: охоронної та пожежної сигналізації; цифрового відеоспостереження; контролю та управління доступом (СКУД) [2, с. 102-103].

Встановлено, що захист інформації від її витоку технічними каналами зв'язку в контексті забезпечення безпекознавчих умов забезпечується: використанням екранованого кабелю та прокладанням проводів і кабелів в екранованих конструкціях; установленням на лініях зв'язку високочастотних фільтрів; побудовою екранованих приміщень ("капсул"); використанням екранованого обладнання; установленням активних систем зашумлення; створенням контрольованої зони. Доведено, що для оцінювання стану технічного захисту інформації, що опрацьовується або циркулює в автоматизованих системах, комп'ютерних мережах, системах зв'язку, та підготовки обґрунтованих висновків для прийняття відповідних рішень проводять експертизу у сфері технічного захисту інформації [3, с. 90-91].

Прорезюмувавши вище описане відзначаємо, що в сучасних умовах турбулентності економічних процесів інформаційна безпека суб'єктів господарювання може бути забезпечена тільки комплексною системою захисту інформації. Комплексна система захисту інформації повинна бути: безперервною, плановою, цілеспрямованої, конкретної, активної, надійною, спиратися на систему різних видів власного програмного забезпечення, здатного реалізувати її функціонування не тільки в повсякденних умовах, але і в критичних ситуаціях.

Список використаних джерел

1. Вівчар О.І. Управління економічною безпекою підприємств: соціогуманітарні контексти: монографія. Тернопіль: ФОП Паляниця В. А., 2018. 474 с.

2. Наконечний В.С. Стан розвитку управління інформаційною безпекою в світовій практиці та її вплив на економічний розвиток України. Сучасний захист інформації. № 4. 2015. С. 100-104.

3. Vivchar O. Contemporary pragmatics and vectors of combating cybercrime in the context of information and economic security strengthening. Актуальні проблеми правознавства. Вип. 2. 2017. С. 86-91.