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.