# Тема 6. Характеристика засобів захисту інформації

Термін «безпека» в електронній комерції означає можливість протистояти спробам нанесення збитків власникам або користувачам системи при різних впливах (навмисних або ненавмисних) на неї.

Під інформаційною безпекою системи електронної комерції розуміють захищеність інформації та інфраструктури, яка її підтримує, від випадкових або навмисних впливів природного чи штучного характеру, здатних нанести збитки власникам або користувачам інформації. Будь-яке порушення безпеки інформації в електронній комерції може бути розглянуте в термінах загроз, уразливості та атак.

З точки зору користувачів, вимоги до безпеки наступні:

* незалежно від механізмів захисту система повинна бути простою, сучасною і надійною, надавати нестандартні рішення складних проблем;
* час передачі даних і сприйняття їх системою повинен бути коротким, щоб користувач мав змогу користуватися всіма функціональними можливостями системи;
* лише особиста інформація повинна бути захищена від несанкціонованого доступу.

Для захисту інтересів суб’єктів інформаційних відносин необхідно забезпечити:

* конфіденційність інформації, яка обробляється системою;
* цілісність компонентів і ресурсів системи та інформації, яка обробляється, накопичується та зберігається;
* доступність компонентів і ресурсів системи.

**Конфіденційність інформації** – це властивість інформації бути доступною тільки суб’єктам системи (користувачам, програмістам, процесам, тощо), які витримали перевірку і були допущені до цієї інформації.

**Цілісність компонентів** – це властивість інформації бути незмінними протягом функціонування системи. Зміни інформації повинні здійснюватися лише авторизованими користувачами.

**Доступність компонентів і ресурсів системи** – це властивість компонентів (ресурсів) системи бути доступними для використання тільки авторизованим користувачам.

Безпека інформаційної системи поділяється на зовнішню і внутрішню. Зовнішня безпека включає:

* захист від втрати або модифікації системи інформації при стихійних лихах;
* захист системи від проникнення зловмисників. Внутрішня безпека включає:
* забезпечення надійної і коректної роботи, цілісності інформації і компонентів системи;
* створення механізмів регламентації діяльності всіх користувачів та обслуговуючого персоналу;
* підтримка дисципліни доступу до системи.

Існує два підходи забезпечення безпеки системи – фрагментарний та комплексний.

**Фрагментарний**, орієнтується на протидію чітко визначеним загрозам при визначених умовах функціонування системи, має міцний захист щодо конкретної загрози безпеки.

**Комплексний** – створює захищене середовище для обробки інформації в системі, яке об’єднує різноманітні правові, організаційні, програмно-технічні засоби протидії будь-яким загрозам.

Захист інформації – це сукупність заходів, які забезпечують перевірку цілісності інформації, виключають або зменшують несанкціонований доступ до інформації, дають змогу відновити інформацію з мінімальними витратами.

Всі заходи та засоби по захисту інформації можна поділити на декілька

груп:

1. Юридичні заходи передбачають наявність законів, які визначають відповідальність осіб, що знищують, пошкоджують інформацію, використовують її без належного дозволу, або сприяють цьому.

До правових заходів відносяться закони про авторські права, статті у кримінальному кодексі, в яких йде мова про пошкодження інформаційних систем. (Закон України «Про Захист інформації в автоматизованих системах»).

1. Адміністративні (організаційні) – це заходи, що регламентують процес функціонування системи, використання її ресурсів, діяльність персоналу, тощо.

До них відносяться: розробка правил обробки інформації, проектування будівель для обробки інформації з урахування впливу зовнішнього середовища, відбір персоналу, організація пропускної системи, організація обліку, зберігання і знищення документів та носіїв конфіденційної інформації, організація розподілу зберігання паролів, криптографічних ключів, сертифікація технічних і програмних засобів.

1. Фізичні заходи захисту включають охорону приміщень, техніки та персоналу, встановлення на дверях приміщень шифрувальних замків, тощо.
2. Технічні засоби передбачають використання пристроїв, які зменшують ймовірність руйнування та викрадання інформації.

Серед найбільш відомих можна назвати блоки безперебійного живлення (UPS), які дозволяють працювати на ЕОМ деякий час після виключення електричного струму, ключі запирання клавіатури, спеціальні комп’ютери разом із специфічним програмним забезпеченням (брандмауери), які обмежують або фільтрують доступ до інформаційної системи із глобальних мереж, електронні картки.

1. Програмні засоби використовуються для визначення та обмеження прав користувачів по доступу до системи, шифрування та розшифровки інформації, що зберігається, фіксування дій користувачів по доступу до системи або інформації, відновлення знищеної інформації на носіях, якщо знищення відбулось на логічному, а не фізичному рівні, тощо.

Подібні програми можуть входити у стандартний комплект поставки того чи іншого програмного продукту загального призначення, або розроблятися під конкретне робоче місце проектувальниками інформаційних систем.

1. Технологічні засоби передбачають включення у технологічний процес спеціальних операцій, які будуть перешкоджати та запобігати пошкодженню, руйнуванню та витоку інформації.

Такі засоби повинні надавати можливість відновити інформацію і програмні засоби з мінімальними витратами часу і праці. Технологічні засоби тісно пов’язані із програмними. Більшість технологічних операцій по захисту інформації вимагають роботи спеціальних програм.

Основні механізми інформаційної безпеки такі:

* управління доступом до інформації;
* ідентифікація та аутентифікація;
* криптографія;
* екранування;
* забезпечення цілісності і доступності даних;
* підтримка працездатності системи електронної комерції при збоях, аваріях, НС;
* відстеження подій, які можуть загрожувати ІБ;
* управління доступом у системах електронної комерції;
* протоколювання дій і подій.

Якщо використовується опис вимог за підсистемами, повинні бути сформульовані додаткові вимоги, регламентовані у вимогах вибраного профілю захисту (класу захищеності системи електронної комерції від несанкціонованого доступу). Можливе використання змішаного підходу, за якого додаткові вимоги описуються в термінах функцій (сервісів) безпеки.