Різновиди шахрайства в електронній комерції:

1. Дані навмисно перехоплюються, читаються або змінюються.
2. Користувачі ідентифікують себе неправильно.
3. Користувач отримує несанкціонований доступ з однієї мережі до іншої.

Засоби захисту інформації:

1. Шифрування інформації. Шифрування використовується для автентифікації і збереження таємниці. Шифрування – метод перетворення первісних даних у закодовану форму. Криптографічні технології (методи захисту даних з використанням шифрування) забезпечують три основних типи послуг для електронної комерції: автентифікацію, неможливість відмови від здійсненого, збереження таємниці. Автентифікація – метод перевірки не тільки особистості відправника, а й наявності чи відсутності змін у повідомленні. Реалізація вимоги неможливості відмови полягає в тому, що відправник не може заперечити, що він відправив певний файл (дані), а отримувач – що він його отримав (це схоже на відправлення замовного листа поштою). Збереження таємниці – захист повідомлень від несанкціонованого перегляду.

В основу шифрування покладено два елементи: криптографічний алгоритм і ключ. Криптографічний алгоритм – математична функція, яка комбінує відкритий текст або іншу зрозумілу інформацію з ланцюжком чисел (ключем) з метою отримати незв'язний (шифрований) текст.

Шифрування з ключем має дві переваги:

* Використовуючи ключ, можна застосовувати той самий алгоритм для відправлення повідомлень різним людям. Головне – закріпити окремий ключ за кожним респондентом.
* Якщо хтось «зламає» зашифроване повідомлення, щоб продовжити шифрування інформації, достатньо лише змінити ключ. Надійність алгоритму шифрування залежить від довжини ключа.

2. Симетричне шифрування або шифрування з таємним ключем. Це найдавніша форма шифрування з використанням ключа. Під час шифрування за такою схемою відправник і одержувач володіють одним ключем, з допомогою якого обидва можуть зашифровувати і розшифровувати інформацію.

Однак існують проблеми з автентичністю, оскільки особистість відправника або одержувача повідомлення гарантувати неможливо.

3. Криптографія з відкритим ключем. Заснована на концепції ключової пари. Кожна половина пари (один ключ) шифрує інформацію так, що її може розшифрувати тільки інша половина (другий ключ). Одна частина ключової пари – особистий ключ – відома тільки її власнику. Інша половина – відкритий ключ – розповсюджується серед усіх його респондентів, але зв'язана тільки з власником. Ключові пари володіють унікальною властивістю: дані, зашифровані будь-яким з ключів пари, можуть бути розшифровані тільки іншим ключем з цієї пари.

Відкрита частина ключової пари може вільно розповсюджуватися, і це не перешкодить використовувати особистий ключ. Ключі можна використовувати і для забезпечення конфіденційності повідомлення, і для автентифікації його автора.

4. Дайджест. Незважаючи на назву, дайджест повідомлення не є його стислим викладенням. Існують криптографічні алгоритми для генерації дайджестів повідомлення – однобічні хеш-функцїі. Однобічна хеш-функція не використовує ключа. Це звичайна формула для перетворення повідомлення будь-якої довжини в один рядок символів (дайджест повідомлення). При використанні 16-байтової хеш-функції оброблений нею текст матиме на виході довжину 16 байтів. Наприклад, повідомлення може бути надане ланцюжком символів VСС349RТУаsdf904. Кожне повідомлення формує свій випадковий дайджест. Якщо зашифрувати дайджест особистим ключем, то можна отримати цифровий підпис.

5. Використання цифрових сертифікатів. Цифровий сертифікат – електронний ідентифікатор, який підтверджує справжність користувача, містить інформацію про нього, слугує електронним підтвердженням відкритих ключів.

Сертифікаційні центри несуть відповідальність за перевірку с особистості користувача, надання цифрових сертифікатів, перевірку їх справжності.

Інші способи захисту інформації:

1. Захист Web-додатків за допомогою S-HTTP i SSL-протоколів.
2. Захист електронної пошти за допомогою стандартів: PEM, S/MINE, PGP.
3. Захист мереж міжмережевими екранами (брандмауери, firewall).

Щодо захисту комерційної інформації їх поділяють на дві групи:

* системи на основі пластикових карток;
* системи на основі цифрових грошей.