**10. Безпека комп’ютерних технологій і систем у банківських установах**

**Мета** – проаналізувати досвід організації комп’ютерних технологій і систем у банківських установах.

**Ключові поняття:**  інформація,технічний захист інформації, система технічного захисту інформації, безпека електронних платежів.

**Основні питання:**

10.1. Система технічного захисту інформації банків.

10.2. Забезпечення безпеки електронних платежів.

***Література:*** [10; 13; 17; 21; 28; 29].

**10.1. Система технічного захисту інформації банків**

В умовах динамічного середовища функціонування банківських установ особливого значення набувають системи технічного захисту інформації.

*Технічні заходи банківської безпеки* – це спрямовані на захист інформації заходи, проведення яких передбачає використання спеціальних технічних засобів, а також реалізацію технічних рішень у сфері банківської безпеки.

*У структуру системи технічного захисту інформації* входять:

об’єкти захисту;

криптографічна підсистема захисту;

підсистема захисту від несанкціонованого доступу.

*Основними об'єктами захисту інформації* є:

технічні та комп’ютерні засоби збору, обробки та зберігання інформації;

програмні засоби та бази даних, що використовуються при зборі, обробці та використанні інформації;

інформація з обмеженим доступом, тобто інформаційні ресурси, зокрема, ті, що містять відомості, які належать або до таємної, або до конфіденційної інформації;

допоміжні технічні засоби і прилади (засоби зв’язку, звукосу­проводження, переговорні і телевізійні пристрої, копіювальна техніка, системи пожежної та охоронної сигналізації, система енергопостачання, радіотрансляційна мережа, енергопобутові прилади тощо, а також самі приміщення, де циркулює інформація.

Підсистема захисту від несанкціонованого доступу будуються на засадах підбору системи технічних заходів, що призначені для закриття каналів витоку інформації. Серед них виділяють:

1) технічні заходи з використанням пасивних методів:

контроль і обмеження доступу на об'єкти й у приміщення;

локалізація випромінювання через екранування, заземлення, звукоізоляцію;

блокування сигналів, що можуть виходити за межі банку через системи опалення, водозабезпечення і каналізації;

установлення автономних або стабілізованих пристроїв електроживлення;

 2) технічні заходи з використанням активних методів:

просторове зашумлення з використанням генераторів шуму, акустичних і вібраційних завад, шумотронів;

лінійне зашумлення мереж електроживлення та кіл заземлення сторонніх дротів та з'єднувальних ліній, що виходять за межі банку;

знешкодження підключених до лінії закладних пристроїв за допомогою спеціальних генераторів імпульсів (випалювачів “жучків”).

*Криптографічна підсистема захисту* полягає в контролі інформаційних потоків шляхом шифрування інформації.

Криптосистеми вирішують такі завдання у сфері інформаційної безпеки:

забезпечення конфіденційності, цілісності даних;

аутентифікацію даних і їх джерел.

Криптографічні методи захисту є гарантією безпечних інформа­ційних систем. Особливе значення криптографічні методи отримали з розвитком розподілених відкритих мереж, в яких немає можливості забезпечити фізичний захист каналів зв'язку. Найнадійніший технічний метод захисту інформації заснований на використанні криптосистем.

Криптографічна система включає:

алгоритм шифрування;

набір ключів (послідовність двійкових чисел), використовуваних для шифрування;

система управління ключами.

Схема роботи криптосистеми полягає в перетворенні тексту в шифртекст за допомогою алгоритму шифрування та ключів, і в зворотному напрямі після передачі зашифрованої інформації.

Класифікація систем шифрування подана в табл. 10.1.

Таблиця 10.1

**Класифікація систем шифрування банківської інформації**

|  |  |
| --- | --- |
| Системи шифрування | Характеристика |
| Спосіб шифрування |
| Cистеми "прозорого" шифрування | Криптографічні перетворення здійснюються в режимі реального часу, непомітно для корис­тувача  |
| Спеціальні системи для шифрування | Програми, які необхідно спеціально виклика­ти для виконання шифрування банківської інформації |
| Ступінь охоплення інформації |
| Канальне шифрування  | Захищається вся інформація, що переда­ється по каналу зв'язку, включаючи службову. Цей спосіб дозволяє досягти вбудовування проце­дур шифрування на канальний рівень і дозво­ляє використо­вувати апаратні засоби, що сприяє підвищенню продуктивності системи захисту банківської інформації |
| Кінцеве (абонентське) шифрування | Дозволяє забезпечити конфіденційність да­них, переданих між двома абонентами. У цьому ви­падку захищається тільки зміст повідомлень, вся службова банківська інформація залишається від­критою |
| Кількість використовуваних ключів |
| Симетричні системи | Використовується один і той же секретний ключ в якості шифратора і дешифратора інформації банку. Недолік цього методу полягає в тому, що ключ повинен бути відомий і відправнику, і одер­жувачу |
| Асиметричні системи | Використовують два взаємопов'язаних ключа: для шифрування й розшифрування. Один ключ є закритим і відомим лише одержувачу. Другий з ключів є відкритим, тобто він може бути за­галь­но доcтупним по мережі і опублікований разом з адресою користувача |

Для контролю електронних платежів використовуються асимет­ричні системи захисту інформації у вигляді електронного цифрового підпису. Він реалізується з використанням методу шифрування з відкритим ключем. Відправник формує цифровий підпис, викори­стовуючи секретний ключ відправника. Одержувач перевіряє підпис, використовуючи відкритий ключ відправника.

Сутність технології електронного підпису полягає в такому: 1) відправник передає два примірники одного повідомлення: відкрите і розшифроване його закритим ключем (тобто зворотне шифрування); 2) одержувач шифрує за допомогою відкритого ключа відправника розшифрований екземпляр; 3) якщо він співпаде з відкритим варіантом, то особистість і підпис відправника вважається встановленою. У процесі використання ЕЦП шифруються не всі повідомлення, а лише спеціальна контрольна сума (хеш), що захищає послання від нелегальної зміни. ЕЦП використовується з метою перевірки цілісності повідомлення та засвідчує особу відправника.

Збережність криптографічних ключів є запорукою безпеки електронних ключів. У разі витоку інформації про криптографічні ключі зловмисник може заволодіти ключовою інформацією й отримати повний доступ до всієї інформації в системі або мережі. Розрізняють такі функцій управління ключами: генерація, зберігання і розподіл ключів (табл. 10.2).

Таблиця 10.2

**Функції управління криптографічними ключами**

|  |  |
| --- | --- |
| Функція | Характеристика |
| Генерація ключів | Для генерації ключів симетричних криптосистем використо­ву­ються апаратні і програмні засоби генерації випадкових чисел. Генерація ключів для асиметричних криптосистем більш склад­на, так як ключі повинні володіти певними математичними властивостями |
| Зберігання ключів | Організація безпечного зберігання, обліку та видалення інформації про криптографічні ключі. Для цього застосовують їх додаткове шифрування за допомогою інших ключів |
| Розподіл ключів | Виконується на основі принципів оперативності, точності, конфі­денційності. Між користувачами мережі ключі розподі­ляють двома способами: за допомогою прямого обміну сеансовими ключами; використовуючи один або декілька центрів розподілу ключів |

В Україні існує затверджений перелік сертифікованих засобів криптографічного захисту інформації. Серед цих засобів:

 Програмний виріб “NovaLib” (Бібліотеки функцій криптографічних перетворень);

Програмний виріб “Шифр” Бібліотеки функцій криптографічних перетворень. Версія 1.0);

Виріб програмний “Шифр+” (Бібліотеки функцій криптографічних перетворень. Версія 1.0);

Програмне забезпечення апаратно-програмних засобів електрон­ного цифрового підпису “Основа”;

Засіб апаратно-програмний криптографічного захисту інформації “Старт”.

**10.2. Забезпечення безпеки електронних платежів**

Для попередження загроз безпеці електронних платежів може використовуватися програмне забезпечення, що відноситься до категорії засобів пошуку «злому» мереж, а саме:

Internet Security Scanner (фірма Internet Security Systems).

NetRecon (фірма Axent).

NetProbe (фірма Qualix).

Ballista (фірма Secure Networks).

NetGuard (фірма Network Guardians).

NetSonar (фірма WheelGroup).

У рамках забезпечення інформаційної безпеки вітчизняні комерційні банки України виступають переважно споживачами спеціального банківського програмного забезпечення іноземного виробництва:

1) комплексну безпеку корпоративних мереж забезпечують програмні продукти VPN ЗАСТАВА 3.3, створені компанією “ЭЛВИС\_ПЛЮС”;

2) криптографічний захист “Крипто Про CSP”, розроблена компанією “Крипто Про”, допомагає ефективно перевіряти електронний цифровий підпис;

3) фінансову безпеку кредиторів забезпечує система A2 AGRUS APPLІCATІON, створена компанією “Агрус MGS”;

4) комплекс “Банк\_Доступ” забезпечує централізоване керування, розподіляючи доступ до інформаційних ресурсів;

5) комплекс “Банк – Активний Захист”, розроблений фірмою “Андек”, використовують для ліквідації наслідків атак хакерів, якщо їм таки удалося прорвати інформаційний захист.

Забезпечення безпеки електронних платежів здійснюється перш за все щодо учасників карткових операцій та електронних платежів.

Система захисту повинна включати захист абсолютно всіх учасників карткових операцій: власників карток, банків, платіжних організацій.

**Етапи забезпечення безпеки карткових операцій** включають:

налагодження взаємодії з правоохоронними органами Українською міжбанківською асоціацією членів EuroPay International (ЄМА), банків­ськими установами з питань ризиків, які виникають у картковому бізнесі, іншими організаціями щодо безпеки карткових проектів;

постановка завдань захисту карткових проектів;

організація ідентифікації клієнтів карткових проектів;

впровадження програм протидії шахрайству;

моніторинг карткових операцій у режимі реального часу;

забезпечення конфіденційності операцій на карткових рахунках;

контроль роботи персоналу задля оперативного виявлення чи недопущення шахрайства;

участь в проведенні розслідувань банківських шахрайств з картковими рахунками.

Найбільш розповсюджені види шахрайств з картковими рахунками:

виготовлення і використання фальшивих банківських карток;

користування вкраденими картками;

злочинні дії персоналу банку щодо списання коштів з карткових рахунків клієнтів;

підробка платіжних документів установами одержувачами платежу.

Інформаційна безпека систем Internet-banking включає два основних напрями інформаційної безпеки:

безпека в системі дистанційного банківського обслуговування (ДБО);

загальна інформаційна безпека банку.

Захист систем ДБО повинен включати:

однозначну ідентифікацію суб'єктів, що взаємодіють із системою (клієнта і банку);

шифрування переданої фінансової інформації;

безпеку каналів передачі інформації, захист носіїв інформації.

Часто в системі Інтернет-банкінг самі клієнти допускають суттєві помилки, а саме:

1. небажане списання коштів через Інтернет-банкінг, що може ста­тися, якщо користувач сам неправильно ввів дані для відправлення грошей;
2. якщо клієнт при відправленні переказу через Інтернет-банкінг до­пустив помилку в номері рахунку, то процедура повернення платежу нічим не відрізняється, від відправлення під час відвідування банку;
3. технічні збої під час виконання операції з переведення грошей;
4. пересилання паролів на неправильний номер телефону.

Розв'язання цих проблем забезпечується професійними засобами захисту, що їх використовують як у західних, так і у вітчизняних системах ДБО. Заходи забезпечення безпеки в системі Інтернет-банкінгу наведено в табл. 10.3.

Таблиця 10.3

**Заходи забезпечення безпеки в системі Інтернет-банкінгу**

|  |  |
| --- | --- |
| Заходи | Характеристика |
| 1 | 2 |
| Створення безпечного середовища функціонування ДБО на стороні клієнтів | Ніякі зміни в робочому коді середовища і його налаштуваннях, що виникли в процесі функціонування системи, не повинні зберігатися при вимиканні системи. У цьому випадку, навіть якщо зловмисник і отримає якимось чином віддалений доступ до цього середовища в процесі його функціонування, він не зможе оволодіти ним на постійній основі |
| Створення захищеного від несанкціонованого доступу каналу передачі інформації між клієнтом і банком | Використовується механізм криптографічної автентифікації сто­рін – для забезпечення захищеної взаємодії через Internet. Забезпе­чення криптографічної автентифікації сторін досягається внаслідок використання захищеного протоколу під час уста­новлення з'єд­нання між Web-сервером банку і клієнтом. Для підтвердження справжності Web-сервера здійснюється порівнян­ня доменного імені сайта банку, що завантажується, з указаним у сертифікаті Web-сервера |

Закінчення табл. 10.3

|  |  |
| --- | --- |
| 1 | 2 |
| Забезпечення безпеки банків­ських серверів, що обслуговують  | Сервери системи Internet-banking, як правило, розміщують в окремому мережевому сегменті з доступом з мережі Internet, що контролюється на міжмережевому екрані (Firewall), і з внутрішньої захищеної мережі банку |
| Забезпечення умов, що не до­пускають розкра­дання ключів і па­ролів, застосову­ваних для роботи в системі ДБО | Ця умова має виконуватися як банком, так і клієнтами. Повернення коштів у випадку користування паролями шахраїв майже неможливе |
| Використання електронного цифрового підпису (ЕЦП) | Електронний цифровий підпис (ЕЦП) – під електронними документами слід використовувати для забезпечення цілісності та автентичності (підтвердження авторства) інформації. ЕЦП клієнта використовується як аналог особистого підпису. Банки мають вести контрольні архіви, в яких зберігаються всі електронні документи з ЕЦП для вирішення конфліктів |
| Шифрування даних  | Слід використовувати для забезпечення конфіденційності інфор­мації, що передається через Internet. Шифрування інформації здійснюється за допомогою сесійних ключів, що генеруються на етапі встановлення з'єднання між клієнтом і Сервером засто­сувань |

В Internet-banking ведеться історія документів – ким і коли документ був створений, відредагований, підписаний, виконаний або відхилений, також ведуться журнали обліку доступу клієнтів по всіх сервісах, у яких зберігається інформація про IP-адресу клієнта, час доступу, ідентифікатор ключа ЕЦП, що був використаний, проведені операції тощо. Під час упровадження системи в банку здійснюється ретельне настроювання операційних систем на серверах Internet-banking –вилучається підтримка протоколів, що не використовуються, мережевих сервісів та служб. Повністю виключається мережевий доступ до файлової системи, задіюються вбудовані в ОС механізми аудиту.

Для захисту системи Інтернет-банкінгу провідні вітчизняні банки використовують: одноразові смс-паролі; зовнішні електронні ключі; одноразові паролі, що отримуються в банкоматі; віртуальну клавіатуру; електронний цифровий підпис.