УДК 004:68

 **ЗАСОБИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ДАНИХ**

*Шевченко В.М., студентка ОС «Бакалавр»*

*Лахно В.А., доктор технічних наук, професор*

*Національний університет біоресурсів і природокористування України*

На першому етапі розвитку концепції забезпечення безпеки інформації, [перевага](http://ua-referat.com/%D0%9F%D0%B5%D1%80%D0%B5%D0%B2%D0%B0%D0%BB) віддавалася програмним засобам захисту. Коли практика показала, що для забезпечення безпеки інформації цього недостатньо, інтенсивний розвиток отримали різноманітні пристрої та системи. У міру формування системного підходу до проблеми забезпечення [інформаційної](http://ua-referat.com/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%8F) безпеки, виникла необхідність комплексного застосування методів захисту та створених на їх основі засобів і [механізмів](http://ua-referat.com/%D0%9C%D0%B5%D1%85%D0%B0%D0%BD%D1%96%D0%B7%D0%BC%D1%96) захисту. Найпростіший і надійний спосіб захисту інформації від загроз несанкціонованого доступу (НСД) - режим автономного використання ПК одним користувачем у спеціально виділеному приміщенні при відсутності сторонніх осіб. У цьому випадку роль замкненого контуру захисту виконує виділене приміщення, а фізичний захист - вікна, стіни, підлога, стеля, двері.

Організаційні заходи захисту засобів комп'ютерної інформації складають сукупність заходів щодо підбору, перевірки та навчання персоналу, який бере участь у всіх стадіях інформаційного процесу. Згідно законодавства України, у державних установах та організаціях можуть створюватись підрозділи, служби, які організують роботу, пов'язану із захистом інформації, підтримкою рівня захисту інформації в автоматизованих системах і несуть відповідальність за ефективність захисту інформації. Однак в банківських установах створення спеціальних структур для захисту інформації, фінансової безпеки є обов'язковим. Деякі фахівці з банківської безпеки пов'язують надійність фінансових інформаційних систем з засобами їх зовнішнього захисту, тобто системою паролів для входу не тільки у саму комп'ютерну мережу, а й до різних рівнів інформації системи, залежно від допуску користувачів. Коло працівників, які за технологією виконання банківських операцій мають доступ до широкого діапазону такої інформації, дуже великий. Тому система захисту, яка базується на кодуванні входів до різних видів інформації, малоефективна. Потрібно знайти принципово нові підходи для розробки та впровадження відносно надійних систем захисту банківської діяльності від комп’ютерних злочинів.

Криптографія вважається одним з найнадійніших способів захисту даних, адже вона охороняє саму інформацію, а не доступ до неї. Криптографічно перетворена інформація має підвищений ступінь захисту зі збереженням підвищеної секретності. З метою захисту інформації при її передачі зазвичай використовують різні методи шифрування даних перед їх введенням до каналу зв'язку або на фізичний носій з наступною розшифровкою. Методи шифрування дозволяють досить надійно захищати комп'ютерну інформацію від злочинних посягань. Застосування криптографічного захисту, тобто кодування тексту з допомогою складних математичних алгоритмів, завойовує все більшу популярність. Звичайно, жоден з шифрувальних алгоритмів не дає цілковитої гарантії захисту від зловмисників, але деякі методи шифрування настільки складні, що ознайомитися зі змістом зашиф­рованих повідомлень практично неможливо.

Криптографічні методи захисту інформації широко використовуються в автоматизованих банківських системах і реалізуються у вигляді апаратних, програмних чи програмно-апаратних методів захисту. Використовуючи шифрування повідомлень в поєднанні з правильною установкою комунікаційних засобів, належними процедурами ідентифікації користувача, можна досягти високого рівня захисту інформаційного обміну. Криптографія є одним з найкращих засобів забезпечення конфіден­ційності і контролю цілісності інформації. Вона займає центральне місце серед програмно-технічних регулювальників безпеки, є основою реалізації багатьох з них і, в той же час, останнім захисним рубежем [1].

Криптографічні методи захисту інформації можуть бути реалізовані як програмними, так і апаратними засобами. HSM (hardware security module) це пристрій (зазвичай у вигляді плати PCI), зі спеціальним крипто процесором, призначений для створення і захисту криптографічних ключів протягом усього циклу їх життя - від генерації до знищення. Всі операції шифрування і розшифрування даних що надходять ззовні відбуваються всередині пристрою. Таким чином, криптографічні ключі ніколи не залишають захищений периметр всередині пристрою, в якому вони були створені. HSM - це свого роду цитаделі, які захищають інформаційні системи для збереження від розкриття цінних даних. Вони захищені від несанкціонованого доступу, фізичного розтину, знімання інформації технічними засобами. HSM забезпечують захист транзакцій, ідентифікаційних даних і додатків, запобігаючи несанкціонованому доступу до найважливішого - криптографічним ключам, за допомогою яких ці дані шифруються. Додатки "звертаються" до HSM за ключами для шифрування / розшифрування даних.

HSM (вельми умовно) поділяються на HSM загального призначення (General Purpose HSM) - Trustway Proteccio, Luna PCIe і HSM призначені для захисту різного роду електронних фінансових транзакцій - платіжні HSM - Trustway Crypt2pay, PayShield.

З точки зору фізичного виконання HSM бувають внутрішні - плати PCI Express, і так звані зовнішні, чи мережеві. Мережеві, як правило, це ті ж самі внутрішні плати встановлені в спеціально захищений від злому корпус з мережевими інтерфейсами. Зовнішній HSM можна встановити в будь-якому місці і використовувати для декількох, географічно рознесених систем, що, з дедалі більшим розширенням додатків, що використовують криптографію, дає суттєву економію. При спробі злому корпусу весь ключовий матеріал знищується, як наслідок, зовнішні HSM мають більш високий клас сертифікації ПО, наприклад, FIPS [2].

Сертифікований високий рівень безпеки, модуля апаратного захисту Trustway Proteccio розроблений (апаратне та програмне забезпечення), впроваджений і повністю виготовлений Atos у Франції. Віртуальний HSM, HSM Trustway Proteccio надає доступ одночасно до 8 віртуальних HSM. Кожен віртуальний HSM - це криптографічний розділ, сильно відокремлений від інших виділеними ключами шифрування, користувачами, адміністраторами та аудиторами. Він пропонує можливість ділитися одним і тим же HSM між різними випадками використання, зберігаючи при цьому однаковий рівень безпеки. Trustway Proteccio постачається із зручним додатком, контрольованим правом доступу для адміністрування, налаштування та управління HSM (політика безпеки, права користувача, управління ключами, конфігурація та оновлення HSM) [3].

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ**

1. Buklib.net [Електронний ресурс]: «Засоби та методи захисту інформації». - Режим доступу: https://buklib.net/books/28625/ (дата звернення: 22.08.2020).

2. Demos.ru [Електронний ресурс]: «Що таке HSM (hardware security module) апаратний модуль безпеки (АМБ)». - Режим доступу: https://www.demos.ru/vendors/crypto/hsm/ (дата звернення: 03.09.2020).

3. Atos.net [Електронний ресурс]: «Шифрування даних за допомогою HSM». - Режим доступу: https://atos.net/en/solutions/cyber-security-products/data-protection-governance/data-encryption-hardware-security-module-hsm (дата звернення: 16.12.2020).