Менеджмент інформаційної безпеки в АБС

Лектор:
Лимаренко Вячеслав Володимирович
к.т. 066-070-8586

Захист інформації в інформаційних системах банківських установ

Як інформаційний об’єкт банк є єдиним комплексом компонентів, пов’язаних між собою єдиною метою, структурними відносинами, технологіями інформаційного обміну. Ці компоненти в процесі функціонування банку можуть змінюватися, на них можуть здійснювати вплив різного роду внутрішні та зовнішні чинники, які складно прогнозувати та оцінювати. Велику кількість компонентів, які формують **банк як об’єкт інформатизації**, можна подати сукупністю чотирьох груп:

- **персонал**
- **технічні засоби інформатизації**
- **програмне забезпечення**
- **документи.**

Ці групи зазнають впливу різного роду специфічних факторів і, взаємодіючи між собою, впливають одна на одну, формуючи відповідний стан інформаційної безпеки банку. Як показує практика, робота з кожною з цих груп щодо забезпечення інформаційної безпеки чи, зокрема, щодо захисту інформації призводить до покращення якості безпеки по одних параметрах і погіршення по інших, що вимагає комплексного підходу до забезпечення інформаційної безпеки банку.

Захист інформації в інформаційних системах банківських установ

Забезпечення інформаційної безпеки і такої її складової, як захист інформації, неможливо здійснити лише організаційними чи технічними заходами, або, скажімо, програмними чи криптографічними.

Дії щодо забезпечення інформаційної безпеки повинні бути регулярним процесом, що здійснюється на всіх напрямах діяльності банку на основі комплексного застосування всіх заходів і засобів безпеки. При цьому засоби, заходи та методи безпеки найбільш раціональним способом об'єднуються в єдиний цілісний механізм не лише для захисту від зловмисників, а й від некомпетентних, недобросовісних працівників банку та різних непередбачуваних ситуацій. Тобто **забезпечення інформаційної безпеки** як і кожної з її складових мусить мати **системний та комплексний характер**.

Системність заходів інформаційної безпеки

Системність заходів інформаційної безпеки має передбачати таке:

- ✓ високий ступінь захищеності інформації банків як головну характеристику її якісного стану;
- ✓ заходами безпеки охоплюються всі інформаційні ресурси банку всієї його структури;
- ✓ діяльність щодо забезпечення інформаційної безпеки є безперервною і плановою, на основі єдиної концепції безпеки;
- ✓ забезпечення інформаційної безпеки здійснюється у тісній єдності з поточною діяльністю банку.

Системність заходів інформаційної безпеки

Комплексний характер системи забезпечує оптимізацію заходів і засобів, що використовуються нею задля створення необхідного балансу вимог і можливостей інформаційної безпеки банку. Комплексний підхід обумовлюється ще й тим, що загрози інформації банку мають різноманітний характер, перекриття яких потребує застосування багатьох, різних за призначенням заходів і засобів.

Забезпечення безпеки у сучасних умовах має здійснюватися як на технологічному, так і на логічному рівнях, що повинно забезпечувати урахування всіх факторів і особливостей, які впливають на безпеку банку, а також усіх компонентів інформаційної роботи:

- Збирання інформації
- Оброблення інформації
- Зберігання інформації
- Передавання інформації
- Використання інформації.

Системність та комплексність банківської безпеки, у тому числі й у сфері захисту інформації є обов’язковою умовою її високої ефективності.

Об’єкти захисту в банку

Основними об’єктами захисту в банку є:

- фінансові ресурси (національна та іноземна валюта, банківські (комерційні) операції та операції банку, коштовності, фінансові документи);
- персонал банку (керівництво і вищий менеджмент банку, особи, які мають доступ до його таємниць, інші працівники банку);
- матеріальні засоби (будівлі, сховища, обладнання, транспорт, засоби і системи інформатизації);
- інформаційні ресурси банку з обмеженим доступом (відомості, що є банківською і комерційною таємницею банку і його конфіденційною інформацією).

Політика безпеки банку

Політика безпеки – це прийнята в банку сукупність норм, правил, рекомендацій згідно з якими будується система його безпеки та управління нею. Вона реалізується за допомогою організаційних заходів і програмнотехнічних засобів, які визначають архітектуру системи захисту та за допомогою засобів управління механізмами захисту. Для кожного конкретного банку політика безпеки є індивідуальною і залежить від особливостей технологій банківського виробництва, змісту інформаційної діяльності та умов роботи банку.

Відповідно до прийнятої в банку політики безпеки проводяться організаційні заходи щодо створення системи захисту інформації.

Система захисту інформації банку – це організована сукупність об'єктів і суб'єктів захисту інформації, заходів, методів і засобів, що використовуються для захисту. Основна мета створення системи захисту інформації – забезпечення надійності зберігання і використання інформації в банку.

Політика безпеки банку

В банках напрацьовано відповідний алгоритм роботи з організації системи захисту інформації, який включає такі дії:

- ✓ визначення вразливості інформації банку (виявлення в інформаційній системі банку місць, використання яких зловмисниками може завдати шкоди інформаційним ресурсам і в цілому банку);
- ✓ визначення мети, завдань та об’єктів захисту інформації;
- ✓ вибір форм, способів і засобів захисту інформації;
- ✓ формування елементів системи захисту інформації, її сил та засобів;
- ✓ створення нормативної бази банку з питань захисту інформації;
- ✓ планування функціонування системи, використання нею сил та засобів захисту інформації у відповідності до особливосте і діяльності банку;
- ✓ забезпечення взаємодії всіх елементів системи між собою та з іншими компонентами, які згідно з політикою безпеки можуть бути задіяні для захисту банківської інформації;
- ✓ забезпечення функціонування системи (матеріальне, фінансове, наукове та ін.);
- ✓ контроль стану захищеності інформації, надійності функціонування системи та ефективності заходів, що вживаються нею.

Система захисту інформації платіжних систем банку

Система захисту інформації платіжних систем банку повинна складатися з:

1) законодавчих актів України та інших нормативно-правових актів, а також внутрішніх нормативних актів суб'єктів переказу, що регулюють порядок доступу та роботи з відповідною інформацією, а також відповідальність за порушення цих правил;
2) заходів охорони приміщень, технічного обладнання відповідної платіжної системи та персоналу суб'єкта переказу;
3) технологічних та програмно-апаратних засобів криптографічного захисту інформації, що обробляється в платіжній системі.

Система захисту інформації платіжних систем банку має забезпечувати:

- цілісність інформації, що передається в платіжній системі, та компонентів платіжної системи;
- конфіденційність інформації під час її обробки, передавання та зберігання в платіжній системі;
- неможливість відмови ініціатора від факту передавання та отримувачем від факту прийняття документа на переказ, документа за операціями із застосуванням засобів ідентифікації, документа на відкликання;
- забезпечення постійного та безперешкодного доступу до компонентів платіжної системи особам, які мають на це право або повноваження, визначені законодавством України, а також встановлені договором.

Цінність інформації

Банки, як правило, не передбачають захисту відкритої інформації.

Але ж відкритість інформації не позбавляє її цінності, а цінна інформація, безумовно, має захищатися, насамперед від втрати її. Захист такої інформації здійснюється за допомогою реєстрації її носіїв, обліку, контролю наявності.

Водночас захист відкритої інформації не повинен обмежувати її загальнодоступність, але доступ до неї має бут и контрольованим із дотриманням відповідних вимог щодо її збереження.

Тобто відкрита інформація є об’єктом захисту, і стосовно неї мають проводитися певні заходи в системі захисту інформації. Загальною ж основою для вибору об’єкта захисту є **цінність інформації**.

Цінність інформації

Критеріями цінності інформації можуть бути:

- необхідність інформації для правового забезпечення діяльності банку;
- необхідність інформації для здійснення виробничої діяльності банку;
- необхідність інформації для ефективного управління діяльністю банку, об'єктивного прийняття управлінських рішень, організації прибуткової діяльності банку;
- необхідність інформації для формування ресурсної бази банку та забезпечення його безпеки.

Цінність інформації

Система захисту інформації банку у своєму функціонуванні має конкретний характер і потребує однозначної конкретизації об'єктів захисту. Інформація, на яку спрямовуються зусилля системи захисту не існує сама по собі, а фіксується (відбивається) у відповідних матеріальних об'єктах або пам'яті людей, тобто вона існує на відповідних носіях.

Обираючи об'єкт захисту, ми маємо визначити певний перелік носіїв невідомої третім особам інформації, за рахунок якої банк отримує певні переваги у своїй діяльності. Це можуть бути відповідні документи, матеріали (у тому числі магнітні, магнітооптичні, оптичні та інші засоби), вироби (засоби відображення, оброблення, відновлення, передання інформації), мережі зв'язку та передання даних, а також працівники банку.

Захист цих об'єктів має здійснюватися регулюванням доступу до них, установленням відповідного порядку їх використання (діяльності) та формуванням умов зберігання. Якраз ці заходи і складають структуру системи захисту інформації.

Цінність інформації

Зазначені заходи в системі захисту інформації проводяться за допомогою технічних, програмних і правових засобів.

До технічних засобів регулювання доступу можна віднести кодовані замки на вході в приміщення, міститься відповідна інформація, установлення засобів і систем пропуску на територію банку, спеціальні прилади та пристрої, що регулюють доступ до інформації, яка зберігається в комп'ютерах.

За допомогою програмних засобів розмежовується доступ до інформації в інформаційних комп'ютерних системах і мережах банку.

Правові засоби є загальними, вони встановлюють як порядок роботи з інформаційними ресурсами банку, так і умови та правила використання технічних і програмних засобів захисту інформації.

Цінність інформації

Вітчизняними банками напрацьовано певний досвід формування нормативно-правової бази з питань захисту інформації.

Насамперед відповідні положення про захист комерційної таємниці включаються до Статуту банку.

Зокрема, у них вказується право банку на:

- ✓ комерційну таємницю;
- ✓ самостійне визначення складу й обсягу відомостей, що становлять комерційну таємницю і конфіденційну інформацію банку;
- ✓ захист комерційної таємниці.

Захист банківських інформаційних систем

При розробленні архітектури та створенні інфраструктури банківської інформаційної системи слід забезпечити її захищеність від загроз. Вирішення цієї проблеми полягає в детальному аналізі таких взаємопов'язаних видів робіт, як проектування та впровадження банківської інформаційної системи, її атестація, аудит та обстеження на предмет безпеки.

З метою забезпечення збереженості конфіденційності, цілісності та доступності інформації, що циркулює в банківських установах, банки мають використовувати у своїй діяльності **спеціалізоване програмно-апаратне забезпечення:**

1. Програмний захист від несанкціонованого входу на робочу станцію комп'ютерної мережі банківської установи;
2. Організації локальної обчислювальної мережі на базі доменної структури. Це дасть змогу адміністратору такої мережі, по-перше, розмежувати права доступу всіх користувачів до певних класів інформації, по-друге, розписати для кожного користувача політику безпеки та організувати його власний профіль, по-третє, обмежити обсяг доступної для збереження інформації з метою збереження сервера від перевантаження та втрати основних властивостей інформації, по-четверте, організувати статистику роботи користувачів у мережі, та у разі необхідності виявити спробу несанкціонованого доступу зловмисника до інформації;

Захист банківських інформаційних систем

3. Програмні модулі мережевого сканування для виконання деяких завдань. Це по-перше, сканування робочих станцій, які ввійшли в мережу, подруге, виявлення несанкціонованої роботи не легалізованих робочих станцій в мережі, по-третє, виявлення нестандартних процесів, завантажених в оперативну пам'ять робочих станцій, по-четверте, виявлення несанкціонованого програмного забезпечення сканування мережі, тощо;

4. Використання серверної платформа та програмні клієнтські модулі управління системою антивірусного захисту. Цей спосіб дає змогу налаштувати автоматичне сканування всієї локальної обчислювальної мережі. Всі основні налаштування, такі як автоматичне щоденне оновлення всіх частин системи антивірусного захисту, автоматичне сканування мережі та робочої станції, тощо, відбуваються на серверній частині програмного забезпечення;

5. Криптозахист файлів електронної пошти банківської установи, які можуть зберігатись на спеціальному поштовому серверів.

Використання всіх перелічених складових дасть змогу забезпечити надійний захист інформації, яка циркулює в автоматизованих системах банківської установи.

Кіберзахист в автоматизованих банківських системах

Згідно із Законом України – Про основні засади забезпечення кібербезпеки України, Національний банк України повинен визначити порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки для суб'єктів переказу коштів, а також здійснювати контроль за їх виконанням.

Національний банк України має намір уперше врегулювати питання щодо забезпечення належного рівня кіберзахисту та інформаційної безпеки у сфері переказу коштів.

Вже розроблено відповідний проект постанови Правління Національного банку України – Про затвердження Положення про кіберзахист та інформаційну безпеку в платіжних системах та системах розрахунків.

Зокрема Проектом постанови передбачено визначити:

- вимоги до суб'єктів платіжного ринку щодо побудови системи захисту інформації та кібербезпеки;
- порядок дій при виявленні кібератак, що знижують надійність функціонування платіжних систем та систем розрахунків;

Кіберзахист в автоматизованих банківських системах

- вимоги до організаційних та технічних заходів з метою забезпечення захисту інформації та кібербезпеки суб'єктами платіжного ринку тощо.

В основу цього документу покладено вимоги і рекомендації національних та міжнародних стандартів з питань інформаційної безпеки, а також загальноприйняті у міжнародній практиці сучасні підходи до забезпечення інформаційної безпеки та кіберзахисту.

Прийняття проекту постанови дасть можливість:

- мінімізувати кількість інцидентів інформаційної безпеки та кіберінциндентів у сфері переказу коштів;
- урегулювати питання використання засобів захисту інформації;
- підвищити надійність функціонування та ефективність платіжних систем і систем розрахунків;
- пришвидшити процес модернізації існуючих платіжних систем з урахуванням сучасних технологій захисту інформації.

Криптографічний захист інформації в автоматизованих банківських системах

Криптографічний захист інформації – це вид захисту, який реалізується за допомогою перетворень інформації з використанням спеціальних (ключових) даних з метою приховування змісту інформації, підтвердження її справжності, цілісності, авторства тощо. Зашифровані повідомлення передаються відкрито, приховується їхній зміст.

Використання криптографічного захисту інформації під час побудови політики безпеки банківської on-line-системи значно посилює безпеку роботи системи, але за умови, що ця система захисту створена належним чином та має безпечну систему розподілу криптографічних ключів.

Криптографічні методи захисту інформації – це методи захисту даних із використанням шифрування.

Шифрування інформації – спосіб маскування конфіденційної інформації; процес перетворення доступних даних на зашифровані (з обмеженим доступом). Процес маскування інформації здійснюється за допомогою спеціального шифру – набору цифр та символів за визначеним алгоритмом, розшифрування якого можливе лише після підбору до нього ключа. Шифрування інформації широко використовується в службах безпеки, банках та інших комерційних підприємствах, що містять дані з обмеженим доступом.

Криптографічний захист інформації в автоматизованих банківських системах

Головна мета шифрування (кодування) інформації – її захист від несанкціонованого читання.

Системи криптографічного захисту (системи шифрування інформації) для банківських on-line-систем можна поділити за різними ознаками:

- за принципами використання криптографічного захисту (вбудований у систему або додатковий механізм, що може бути відключений);
- за способом реалізації (апаратний, програмний, програмно-апаратний);
- за криптографічними алгоритмами, які використовуються (загальні, спеціальні);
- за цілями захисту (забезпечення конфіденційності інформації (шифрування) та захисту повідомлень і даних від модифікації, регулювання доступу та привілеїв користувачів);
- за методом розподілу криптографічних ключів (базових/сеансових ключів, відкритих ключів) тощо.

Вбудовані механізми криптографічного захисту входять до складу системи, їх створюють одночасно з розробленням банківської on-line-системи. Такі механізми можуть бути окремими компонентами системи або бути розподіленими між іншими компонентами системи.

Криптографічний захист інформації в АБС

За способом реалізації криптографічний захист можна здійснювати різними способами: апаратним, програмним або програмно-апаратним.

Апаратна реалізація криптографічного захисту – найбільш надійний спосіб, але й найдорожчий. Інформація для апаратних засобів передається в електронній формі через порт обчислювальної машини всередину апаратури, де виконується шифрування інформації. Перехоплення та підробка інформації під час її передавання в апаратуру може бути виконана за допомогою спеціально розроблених програм типу – вірус.

Програмна реалізація криптографічного захисту є значно дешевшою та гнучкішою в реалізації. Але виникають питання щодо захисту криптографічних ключів від перехоплення під час роботи програми та після її завершення. Тому, крім захисту від вірусних атак, потрібно вжити заходів для забезпечення повного звільнення пам'яті від криптографічних ключів, що використовувались під час роботи програм – збирання сміття.

Крім того, можна використовувати **комбінацію апаратних і програмних механізмів криптографічного захисту.** Найчастіше використовують програмну реалізацію криптоалгоритмів з апаратним зберіганням ключів. Такий спосіб криптозахисту є досить надійним і не надто дорогим. Але, вибираючи апаратні засоби для зберігання криптографічних ключів, треба пам’ятати про забезпечення захисту від перехоплення ключів під час їх зчитування з носія та використання.

Криптографічний захист інформації в АБС

В основу шифрування покладено два елементи: криптографічний алгоритм і ключ.

Криптографічний алгоритм – це математична функція, яка комбінує відповідний текст або іншу зрозумілу інформацію з ланцюжком чисел (ключем) з метою отримання незв'язаного (шифрованого) тексту. Криптографічні алгоритми застосовують із метою:

- шифрування інформації;
- захисту даних і повідомлень (інформації) від модифікації або підробки.

Усі криптографічні алгоритми можна поділити на дві групи: загальні і спеціальні.

Спеціальні криптографічні алгоритми мають секретний алгоритм шифрування, а загальні криптографічні алгоритми характеризуються повністю відкритим алгоритмом, і їх криптостійкість визначається ключами шифрування. Спеціальні алгоритми найчастіше використовують в апаратних засобах криптографічного захисту.

Загальні криптографічні алгоритми часто стають стандартами шифрування, якщо їхню висока криптостійкість доведено. Ці алгоритми оприлюднюють для обговорення, при цьому навіть визначається премію за успішну спробу його зламування. Криптостійкість загальних алгоритмів визначається ключем шифрування, який генерується методом випадкових чисел і не може бути повторений протягом певного часу. Криптостійкість таких алгоритмів буде вищою зі збільшенням довжини ключа.

Криптографічний захист інформації в АБС

Є дві великі групи загальних криптографічних алгоритмів: симетричні і асиметричні.

До **симетричних криптографічних алгоритмів** належать такі алгоритми, для яких шифрування і розшифрування виконується однаковим ключем, тобто і відправник і отримувач повідомлення мають користуватися тим самим ключем. Такі алгоритми мають досить велику швидкість оброблення як для апаратної, так і для програмної реалізації. Основним їх недоліком є труднощі, пов'язані з дотриманням безпечного розподілу ключів між абонентами системи.

Для **асиметричних криптографічних алгоритмів** шифрування і розшифрування виконують за допомогою різних ключів, тобто, маючи один із ключів, не можна визначити парний для нього ключ. Такі алгоритми часто потребують значно довшого часу для обчислення, але не створюють труднощів під час розподілу ключів, оскільки відкритий розподіл одного з ключів не зменшує криптостійкості алгоритму і не дає можливості відновлення парного йому ключа.

Криптографічний захист інформації в АБС

Найбільш поширеним є стандарт шифрування даних **DES (Data Encryption Standart)** та алгоритм **RSA**, названий за першими літерами прізвищ розробників (Rivest, Shamir, Adleman), розроблені у 1970-х роках. Обидва алгоритми є державними стандартами США. DES є симетричним алгоритмом, а RSA – асиметричним. Ступінь захищеності під час використання цих алгоритмів прямо залежить від довжини ключа, що застосовується.

Ще одним алгоритмом, що широко застосовується, зокрема, в банківській системі, є алгоритм **Діффі-Геллмана**.

Алгоритм Діффі-Геллмана (Diffie–Hellman key exchange (D–H)) – це метод обміну криптографічними ключами. Один з перших практичних прикладів обміну ключами, що дозволяє двом учасникам, що не мають жодних попередніх даних один про одного, отримати спільний секретний ключ із використанням незахищеного каналу зв'язку. Цей ключ можна використати для шифрування наступних сеансів зв'язку, що використовують шифр з симетричним ключем. Схему вперше оприлюднили Вітфілд Діффі і Мартін Геллман у 1976 році.

Хоча протокол Діффі-Геллмана є анонімним (без автентифікації) протоколом встановлення ключа, він забезпечує базу для різноманітних протоколів з автентифікацією, і використовується для забезпечення цілковитої прямої секретності в недовговічних режимах Transport Layer Security (відомих як EDH або DHE залежно від комплектації шифру).

Криптографічний захист інформації в АБС

Алгоритм **DSA** (Digital Signature Algorithm) – криптографічний алгоритм з використанням відкритого ключа для створення електронного підпису, але не для шифрування (на відміну від RSA і схеми Ель-Гамаля). Підпис створюється таємно, але може бути публічно перевірений. Це означає, що тільки один суб'єкт може створити підпис повідомлення, але будь-хто може перевірити її коректність.

Алгоритм **Advanced Encryption Standard (AES)** – симетричний алгоритм блочного шифрування (розмір блока 128 біт, ключ 128/192/256 біт), фіналіст конкурсу AES і прийнятий як американський стандарт шифрування урядом США.

Усі криптографічні алгоритми можна використовувати з різною метою, зокрема:

- для шифрування інформації, тобто приховування змісту повідомлень і даних;
- для забезпечення захисту даних і повідомлень від модифікації.

Криптографічний захист інформації в АБС

Для приховування інформації можна використовувати деякі асиметричні алгоритми, наприклад, алгоритм RSA. Алгоритм підтримує змінну довжину ключа та змінний розмір блоку тексту, що шифрується.

Алгоритм RSA дає змогу виконувати шифрування в різних режимах:

- за допомогою секретного ключа відправника. Тоді всі, хто має його відкритий ключ, можуть розшифрувати це повідомлення;
- за допомогою відкритого ключа отримувача, тоді тільки власник таємного ключа, який є парним до цього відкритого, може розшифрувати таке повідомлення;
- за допомогою секретного ключа відправника і відкритого ключа отримувача повідомлення. Тоді тільки цей отримувач може розшифрувати таке повідомлення.

Не всі асиметричні алгоритми дозволяють виконувати шифрування даних у таких режимах. Це визначається математичними функціями, які закладені в основу алгоритмів.

Криптографічний захист інформації в АБС

Іншою метою використання криптографічних методів є захист інформації від модифікації, викривлення або підроблення. Цього можна досягнути без шифрування повідомлень, тобто повідомлення залишається відкритим, незашифрованим, але до нього додається інформацію, перевірка якої за допомогою спеціальних алгоритмів може однозначно довести, що ця інформація не була змінена.

Для симетричних алгоритмів шифрування така додаткова інформація – це код автентифікації, який формується за наявності ключа шифрування за допомогою криптографічних алгоритмів.

Для асиметричних криптографічних алгоритмів формують додаткову інформацію, яка має назву **електронний цифровий підпис** (сукупність даних, які дають змогу підтвердити цілісність електронного документа та ідентифікувати особу, яка його підписала.).

Криптографічний захист інформації в АБС

Формуючи електронний цифровий підпис, виконують такі операції:

- за допомогою односторонньої хеш-функції обчислюють прообраз цифрового підпису, аналог контрольної суми повідомлення;
- отримане значення хеш-функції шифрується:
  - ✓ таємним або відкритим;
  - ✓ таємним і відкритим ключами відправника і отримувача повідомлення – для алгоритму RSA;
- використовуючи значення хеш-функції і секретного ключа, за допомогою спеціального алгоритму обчислюють значення цифрового підпису.

Криптографічний захист інформації в АБС

Для того, щоб перевірити цифровий підпис, потрібно:

- виходячи із значення цифрового підпису та використовуючи відповідні ключі, обчислити значення хеш-функції;
- обчислити хеш-функцію з тексту повідомлення;
- порівняти ці значення. Якщо вони збігаються, то повідомлення не було модифікованим і відправлене саме цим відправником.

Останнім часом використання електронного цифрового підпису значно поширюється, у тому числі для регулювання доступу до конфіденційної банківської інформації та ресурсів системи, особливо для on-line-систем реального часу.

Криптографічний захист інформації в АБС

Ефективність захисту систем за допомогою будь-яких криптографічних алгоритмів значною мірою залежить від безпечного розподілу ключів. Ссновні методи розподілу ключів між учасниками системи:

1. **Метод базових/сеансових ключів.** Цей метод описано у стандарті ISO 8532 і використовується для розподілу ключів симетричних алгоритмів шифрування. Для розподілу ключів вводиться ієрархія ключів: головний ключ (так званий майстер-ключ, або ключ шифрування ключів) і ключ шифрування даних (тобто сеансовий ключ). Ієрархія може бути і дворівневою: ключ шифрування ключів/ключ шифрування даних. Старший ключ у цій ієрархії треба розповсюджувати неелектронним способом, який виключає можливість його компрометації. Використання такої схеми розподілу ключів потребує значного часу і значних затрат.
2. **Метод відкритих ключів.** Цей метод описано у стандарті ISO 11166 і його може бути використано для розподілу ключів як для симетричного, так і для асиметричного шифрування. За його допомогою можна також забезпечити надійне функціонування центрів сертифікації ключів для електронного цифрового підпису на базі асиметричних алгоритмів та розподіл сертифікатів відкритих ключів учасників інформаційних систем. Крім того, використання методу відкритих ключів дає можливість кожне повідомлення шифрувати окремим ключем симетричного алгоритму та передавати цей ключ із самим повідомленням у зашифрованій асиметричним алгоритмом формі.

Криптографічний захист інформації в АБС

Вибір того чи іншого методу залежить від структури системи і технології обробки даних. Жоден із цих методів не забезпечує абсолютного захисту інформації, але гарантує, що вартість зламування у кілька разів перевищує вартість зашифрованої інформації.

Для використання системи криптографії з відкритим ключем потрібно генерувати відкритий і особистий ключі. Після генерування ключової пари слід розповсюдити відкритий ключ респондентам. Найнадійніший спосіб розповсюдження відкритих ключів – через сертифікаційні центри, що призначені для зберігання цифрових сертифікатів.

Цифровий сертифікат – це електронний ідентифікатор, що підтверджує справжність особи користувача, містить певну інформацію про нього, слугує електронним підтвердженням відкритих ключів.

Загалом, для забезпечення належного рівня захищеності інформації потрібна **криптографічна система** – сукупність засобів криптографічного захисту, необхідної ключової, нормативної, експлуатаційної, а також іншої документації (зокрема й такої, що визначає заходи безпеки).

Головним обмеженням криптографічних систем є те, що при одержанні повідомлення зашифрованого парним ключем, не можна дізнатися напевне, хто саме його відправив.

Криптографічний захист інформації в АБС

Постановою правління Національного банку України від 28.09.2017 № 95 Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України визначено такі **принципи криптографічного захисту інформаційних систем Національного банку України**:

1. Криптографічний захист інформації в інформаційних системах Національного банку України на ділянці зв'язку між учасником інформаційних систем Національного банку та Національним банком забезпечується застосуванням багаторівневого (ешелонованого) підходу, за яким окремо за допомогою незалежних систем криптографічного захисту інформації захищається сеансів рівень базової еталонної моделі взаємодії відкритих систем (Open systems interconnection basic reference model, OSI/ISO) та прикладний рівень моделі взаємодії відкритих систем інформаційних систем Національного банку;

Криптографічний захист інформації в АБС

2. Для захисту сеансового рівня моделі взаємодії відкритих систем інформаційних систем Національного банку використовується криптографічний протокол захисту на транспортному рівні (Transport layer security, TLS), забезпечуються контроль цілісності та конфіденційність інформації. Для прикладного рівня моделі взаємодії відкритих систем інформаційних систем Національного банку використовуються такі механізми захисту:

- ✓ ідентифікація/автентифікація підписувача
- ✓ контроль цілісності
- ✓ конфіденційність на всіх етапах оброблення інформації;

3. Залежно від категорії інформації щодо критерію конфіденційності, для забезпечення ідентифікації та автентифікації, використовується односпрямований (криптографічний ключ лише на стороні сервера, сувора криптографічна автентифікація сервера) або двоспрямований достовірний канал захисту на транспортному рівні (криптографічний ключ на стороні клієнта і на стороні сервера, сувора криптографічна автентифікація обох сторін з'єднання).

Криптографічний захист інформації в АБС

Цією постановою також визначено такі обов’язкові заходи щодо криптографічного захисту інформації в інформаційних системах Національного банку України:

– налаштувати системи криптографічного захисту інформації в інформаційних системах Національного банку згідно з вимогами, які визначені у відповідній експлуатаційній документації кожної інформаційної системи Національного банку;

– забезпечити захист інформаційних систем банку від несанкціонованого доступу та дій, спрямованих на відмову в обслуговуванні.

Криптографічний захист інформації в АБС

У разі застосування криптографічного захисту банк зобов'язаний використовувати криптографічні алгоритми з такого переліку:

1) асиметричні алгоритми:

- алгоритм Діффі-Геллмана (алгоритм DH) для узгодження сеансових ключів шифрування;
- алгоритм цифрового підпису (алгоритм DSA) для цифрових підписів;
- алгоритм Діффі-Геллмана на еліптичних кривих (алгоритм ECDH) для узгодження сеансових ключів шифрування;
- алгоритм цифрового підпису на еліптичних кривих (алгоритм ECDSA) для цифрових підписів;
- алгоритм Ривест-Шаміра-Адлемана (алгоритм RSA) для цифрових підписів і узгодження сеансових ключів шифрування або аналогічних ключів;
- алгоритм цифрового підпису (ДСТУ 4145-2002 Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння для цифрових підписів;

Криптографічний захист інформації в АБС

2) алгоритми безпеки хешування SHA-224, SHA-256, SHA-384, SHA-512, Купина (ДСТУ 7564:2014 Інформаційні технології. Криптографічний захист інформації. Функція хешування) або більш криптостійкі;

3) алгоритми симетричного шифрування:

- алгоритм Advanced encryption standard (AES) із використанням довжини ключа 128, 192 і 256 біт або більше;
- алгоритм криптографічного перетворення (ДСТУ ГОСТ 28147:2009 Система оброблення інформації. Захист криптографічний. Алгоритм криптографічного перетворення);
- алгоритм Калина (ДСТУ 7624:2014 Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення).

Криптографічний захист інформації в АБС

Банк зобов’язаний використовувати останню версію протоколу захисту на транспортному рівні та реалізацію цього протоколу, що підтримує безпечне повторне погодження з’єднання для захисту з’єднань, які управляються протоколом Transmission control protocol (TCP).

Якщо безпечне повторне погодження з’єднання не підтримується, то ця процедура має бути відключена.

Криптографічний захист інформації та заходи захисту інформаційної безпеки в платіжних системах банку

Використання криптографічного захисту інформації під час розроблення політики платіжної системи як складової політики інформаційної безпеки значно посилює безпеку роботи системи.

За принципами використання криптографічний захист може бути вбудованим у платіжну систему або бути додатковим механізмом, який може відключатися. Використовуються дві групи криптографічних алгоритмів:

1) загальні:

- симетричні;
- асиметричні;

2) спеціальні.

Криптографічний захист інформації та заходи захисту інформаційної безпеки в платіжних системах банку

Особливу увагу потрібно приділити методам розподілу криптографічних ключів між учасниками платіжної системи, а саме методом:

- базово-сеансових ключів;
- відкритих ключів.

Апаратно-програмні засоби криптографічного захисту інформації в системі банківських платежів забезпечують автентифікацію відправника та отримувача електронних банківських документів і службових повідомлень системи банківських платежів, гарантують їх достовірність та цілісність, неможливість підроблення або викривлення документів у шифрованому вигляді та за наявності електронного цифрового підпису.

Криптографічний захист інформації та заходи захисту інформаційної безпеки в платіжних системах банку

Криптографічний захист інформації охоплює всі етапи оброблення електронних банківських документів з часу їх створення до зберігання в архівах банку. Використання різних криптографічних алгоритмів на різних етапах оброблення електронних банківських документів дає змогу забезпечити безперервний захист інформації в системі банківських платежів. Криптографічний захист інформації гарантує цілісність та конфіденційність електронної банківської інформації, а також сувору автентифікацію учасників системи банківських платежів і їх фахівців, які здійснюють підготовку та оброблення електронних банківських документів.

Для здійснення суворої автентифікації банків (філій), які є учасниками системи банківських платежів, застосовують систему ідентифікації користувачів, яка є основою системи розподілу ключів криптографічного захисту. Учасник системи електронних платежів (СЕП) для забезпечення захисту інформації має трибайтові ідентифікатор, перший знак якого є літерою відповідної території, на якій він розташований; другий та третій знаки є унікальними ідентифікаторами учасника СЕП у межах цієї території. Ідентифікатори мають бути узгодженими з адресами СЕП і бути унікальними у межах банківської системи України.

Криптографічний захист інформації та заходи захисту інформаційної безпеки в платіжних системах банку

Трибайтові ідентифікатори є складовою частиною ідентифікаторів ключів криптографічного захисту для робочих місць системи автоматизації банку, де формуються та обробляються електронні банківські документи. Ідентифікатор ключів криптографічного захисту для робочих місць складається з шести символів, з яких три перші є ідентифікаторами учасника системи електронних платежів, четвертий – визначає тип робочого місця (операціоніст, бухгалтер тощо), п’ятий і шостий – ідентифікатор конкретного робочого місця (тобто службовця, який відповідає за оброблення електронних банківських документів на цьому робочому місці). Трибайтовий ідентифікатор учасника СЕП убудований у програму генерації ключів і не може бути змінено учасником СЕП, що забезпечує захист від підроблення ключів від імені інших учасників СЕП. Ідентифікатори ключів записуються в апаратуру криптографічного захисту інформації (АКЗІ), яка надається учасникам СЕП і забезпечує апаратне формування (перевірку) електронного цифрового підпису та апаратне шифрування (розшифрування) на АРМ-НБУ.

Криптографічний захист інформації та заходи захисту інформаційної безпеки в платіжних системах банку

Фізичний захист систем електронних платежів потребує виконання вимог щодо безпечного та надійного функціонування ключових обчислювальних машин платіжної системи.

Особливої охорони і захисту потребують центри генерації та сертифікації ключів платіжної системи. Вони повинні бути обладнані відповідною обчислювальною технікою, яка пройшла дослідження на побічні електромагнітні випромінювання для захисту від перехоплення і витоку ключової інформації технічними каналами. Обчислювальна техніка для генерації і сертифікації ключів не повинна входити до локальних мереж центрального банку або повинна бути обладнана відповідною системою захисту від втручання з інших робочих місць локальної мережі. Доступ до приміщень центру генерації і сертифікації ключів повинен бути суворо обмеженим.


Дякую за увагу
Лекцію закінчено