

Системи електронного обміну даними

Лектор:

Лимаренко Вячеслав Володимирович

к.т. 066-070-8586

Вимоги до інформаційної безпеки телекомунікаційних систем кредитно-фінансової сфери

Інформаційне середовище взагалі та кредитно-фінансова сфера зокрема є надзвичайно привабливими для кримінальних структур. В останні десятиріччя зростання збитків, пов'язане з інформаційною злочинністю, стало стійкою тенденцією. Телекомунікаційне середовище повинно за вимогами ISO (Міжнародна організація стандартизації) забезпечувати:

- ☐ захист інформації (з метою забезпечення її конфіденційності, цілісності та вірогідності) при її зберіганні, обробці та передачі по мережах;
- ☐ підтвердження справжності даних і користувачів (автентифікація сторін, що встановлюють зв'язок);
- ☐ виявлення та попередження порушення цілісності даних;

Вимоги до інформаційної безпеки телекомунікаційних систем кредитно-фінансової сфери

- ❑ захист технічних засобів і приміщень, в яких обробляється конфіденційна інформація, від витоку інформації за сторонніми каналами і від можливо впроваджених у технічні засоби електронних пристроїв знімання інформації;
- ❑ захист програмних продуктів від впровадження програмних закладок і «вірусів»;
- ❑ захист від несанкціонованого доступу до інформаційних ресурсів і технічних засобів мережі, у тому числі і до засобів її управління, з метою запобігання зниженню рівня захищеності інформації та самої мережі в цілому;
- ❑ реалізацію організаційно-технічних заходів, спрямованих на забезпечення збереження конфіденційних даних.

Вимоги до інформаційної безпеки телекомунікаційних систем кредитно-фінансової сфери

Для реалізації зазначених вимог інформаційної безпеки використовується комплекс апаратно-програмних та організаційно-технічних заходів, що реалізують систему безпеки у вигляді розподіленого комплексу, який функціонує під керівництвом *центрів управління безпекою* (ЦУБ) мережі.

Для систем передачі економічно значущої інформації системи захисту інформації під час передачі відкритими каналами зв'язку повинні забезпечувати захист від такого:

- ☐ несанкціонованого доступу до переданих повідомлень (перешкоджати порушенню конфіденційності);
- ☐ навмисної зміни одержувачем повідомлення з метою дискредитації відправника або комунікаційної компанії;

Вимоги до інформаційної безпеки телекомунікаційних систем кредитно-фінансової сфери

- ☐ видачі одного користувача системою за іншого, щоб зняти із себе відповідальність або ж використати його повноваження з метою формування помилкового повідомлення, зміни законного, санкціонування помилкових обмінів повідомленнями або ж їх підтвердження;
- ☐ відмови від факту формування та передачі повідомлення;
- ☐ твердження про те, що повідомлення отримане від деякого користувача, хоча насправді воно сформовано самим зловмисником;
- ☐ твердження про те, що одержувачу в заданий момент часу було надіслане повідомлення, яке насправді не відсилося (або відсилося в інший момент часу);
- ☐ відмови від факту одержання повідомлення, що насправді було отримано, або видачі

Вимоги до інформаційної безпеки телекомунікаційних систем кредитно-фінансової сфери

- ❑ несанкціонованої зміни повноважень інших користувачів на відправлення та одержання повідомлень (помилковий запис інших осіб, обмеження або розширення встановлених повноважень тощо);
- ❑ набору статистики обміну повідомленнями (вивчення того, хто, коли і до яких повідомлень має доступ);
- ❑ заяви про сумнівність протоколу забезпечення безпеки доставки повідомлень через розкриття певної конфіденційної інформації;
- ❑ введення зловмисником помилкових доручень і службової інформації;
- ❑ створення перешкод у каналах зв'язку з метою виключення можливості доведення повідомлення до одержувача.

Вимоги до інформаційної безпеки телекомунікаційних систем кредитно-фінансової сфери

Обмеження при побудові систем інформаційної безпеки в кредитно-фінансових організаціях такі:

- ☐ витрати на побудову систем захисту не повинні перевищувати величину гіпотетично передбачуваного збитку;
- ☐ політика відкритості суперечить політиці забезпечення інформаційної безпеки.

Системи передачі банківських повідомлень

Діючі нині електронні системи передачі банківських повідомлень можна поділити на *системи фінансових повідомлень* і *системи розрахунків*.

Системи фінансових повідомлень — здійснюється тільки оперативне пересилання і зберігання міжбанківських документів. До системи належать S.W.I.F.T., Bank Wire (приватна мережа банків США) тощо.

Системи розрахунків — функції пов'язані безпосередньо з виконанням взаємних вимог і зобов'язань. До системи належать CHIPS (США), CHAPS (Англія) та ін.

Системи передачі банківських повідомлень

Спеціальна мережа передачі банківських повідомлень на міжнародному рівні **S.W.I.F.T.** (Society for Worldwide Interbank Financial Telecommunications) – одна з найбільших у світі систем банківських повідомлень.

Мета створення цієї «Міжнародної міжбанківської організації валютних і фінансових розрахунків по телексу» – забезпечення всім учасникам доступу до цілодобової високошвидкісної мережі передачі банківської інформації в стандартній формі за високого ступеня контролю і захисту від несанкціонованого доступу.

Акціонерне товариство S.W.I.F.T. зі штаб-квартирою в Бельгії засноване в Брюсселі в 1973 р. групою європейських і північноамериканських банків, перебуває під юрисдикцією права Бельгії і належить банкам-членам товариства. Першими членами S.W.I.F.T. стали 239 банків із 15 країн. Висока надійність системи, підтримка провідних банків світу, стабільна продуктивність, високий рівень стандартизації зумовили незмінне зростання її популярності. Переваги S.W.I.F.T. стали настільки очевидними для банків, що аналогічні системи (лондонська автоматична платіжна система розрахункових палат CHAPS, французька Sagitaire, нью-йоркська CHIPS) створили систему автоматичного переведення стандартів S.W.I.F.T. у власні. На цей час вона має модифікацію **S.W.I.F.T. II**. Вона базується на *чотирирівневій мережній архітектурі*. Логічна архітектура системи відповідає основним принципам ISO для взаємодії відкритих систем.

Архітектура S.W.I.F.T.

Кожний активний компонент архітектури S.W.I.F.T. II називається вузлом. Вузли можуть бути зв'язані між собою:

- прямими виділеними лініями;
- місцевими та міжнародними лініями з комутацією;
- локальними мережами;
- супутниковими каналами зв'язку.

Для керування в системі задіяно чотири типи процесорів (логічних):

- ☐ SCP (System Control Processor) – процесор керування системою;
- ☐ SP (Settlement Processor) – комутаційний процесор;
- ☐ RP (Regional Processor) – регіональний процесор;
- ☐ CP (Communication Processor) – процесор передачі.

Архітектура S.W.I.F.T.

Процесор керування системою SCP відповідає за функціонування всієї системи загалом. Він постійно контролює та керує всіма активними компонентами системи і доступом до системи в цілому. До функцій керування SCP належать:

- дозвіл відкриття нового сеансу та збереження даних сеансу;
- поширення нового програмного забезпечення у системі;
- функціональний контроль усіх технічних і програмних засобів;
- збирання діагностичної інформації щодо несправностей;
- керування процесом відновлення після помилки;
- динамічний розподіл системних ресурсів.

Архітектура S.W.I.F.T.

Комутаційні процесори SP керують маршрутизацією та зберіганням повідомлень. Їх основні функції такі:

- маршрутизація повідомлень між користувачами через регіональні процесори RP;
- надійне зберігання двох копій усіх оброблених певним комутаційним процесором повідомлень (на двох різних носіях) і відповідної їм передісторії доставки;
- формування підтверджень про зберігання, доставку оброблених певним комутаційним процесором повідомлень або їх ненадходження;
- обробка вибірки повідомлень.

Архітектура S.W.I.F.T.

Регіональний процесор RP здійснює логічне підключення користувачів до мережі S.W.I.F.T. і, по суті, є вхідною та вихідною точками системи. Програмне забезпечення RP, взаємодіючи із програмами користувача, здійснює точне і безпечне логічне підключення до S.W.I.F.T.

До його функцій належать:

- перевірка вхідних повідомлень перед пересиланням до комутаційного процесора;
- обробка протоколів прикладного рівня;
- контроль і перевірка номерів вхідної послідовності (ISN) усіх повідомлень;
- верифікація контрольних сум повідомлень;
- формування позитивних (ACK) і негативних (NAK) підтверджень прийому повідомлень.

Архітектура S.W.I.F.T.

Процесор передачі CP забезпечує зв'язок між регіональними процесорами RP та іншими вузлами системи, тим самим дозволяючи RP, підключеному до власного комутаційного процесора SP, приймати інформацію від інших SP.

Кожний регіональний процесор обслуговує конкретну країну або територію та розташований у безпечних (з контролем доступу) центрах. Для кожного користувача системи, відомого за його фізичною адресою, призначається його основний регіональний процесор RP, що і обслуговуватиме цього користувача.

Фактично вся система S.W.I.F.T. II зосереджена в двох центрах управління системою (SCC), які розташовані в Нідерландах і США.

SCC містить у собі два ключові компоненти системи, а саме – процесор керування системою SCP і комутаційний процесор SP. Для поліпшення працездатності та захисту від перебоїв у системі S.W.I.F.T. II застосовується дублювання кожного SCP і резервування роботи кожного SP. У будь-який час тільки один процесор керування системою є активним і здійснює безпосереднє керування системою. Інші три SCP постійно перебувають у резерві та безперервно обновляють свій стан за даними конфігурації активного SCP.

Підключення до S.W.I.F.T.

Для того, щоб одержати фізичний доступ до системи S.W.I.F.T. індивідуальні користувачі повинні мати комп'ютерний термінал (CBT), що підключається до системи S.W.I.F.T. через ряд локальних вузлів підключення, відомих як точки доступу до системи S.W.I.F.T. (SAP) або віддалені точки доступу (RAP). До складу SAP/RAP входять:

- процесор, що виконує функції керування лініями користувача та лініями підключення SAP/RAP до транспортної мережі S.W.I.F.T. II (STN);
- порти, надані користувачам.

Доступ до послуг S.W.I.F.T. II через SAP або RAP забезпечується транспортною мережею STN, що працює за комунікаційним протоколом X.25. Розходження між SAP та RAP полягає в забезпеченні рівня безпеки, хоча вони забезпечують однакові операційні можливості щодо роботи з кількома окремо підключеними користувачами. Якщо через проблеми на лінії зв'язку або несправності SAP (RAP) користувач не може увійти до системи в його основній точці доступу SAP (RAP), то альтернативний вхід до системи може бути зроблений в іншій точці доступу.

Підключення до S.W.I.F.T.

Підключення користувачів до мережі S.W.I.F.T. можливе за виділеними лініями зв'язку через загальні мережі передачі даних (PDN) або через лінії з комутацією (PSTN), підключені до точки доступу. Підключення виділених ліній доступне у всіх SAP зі швидкістю передачі даних 2400, 4800 та 9600 біт/с. При цьому типі підключення користувачеві виділяється окремий порт у точці доступу та може бути використане шифрування (за бажанням користувача).

Підключення через PDN можливе тільки зі швидкостями, еквівалентними швидкостям виділених ліній. Підключення користувача до PDN забезпечується за допомогою виділених ліній з використанням протоколу X.25. Для цього типу підключення передбачається обов'язкове шифрування даних відповідно до протоколу X.25.

У системі S.W.I.F.T. II є два типи підключення через лінії з комутацією:

- ☐ через порти PSTN спільного використання, до яких всі користувачі мають доступ на основі суворої конкуренції. Швидкість роботи через ці порти не більше 2400 біт/с і засоби шифрування не застосовуються;
- ☐ через виділені порти (для кожного користувача окремий) зі швидкістю передачі даних до 9600 біт/с і можливістю (за бажанням користувача) застосовувати засоби шифрування інформації.

Безпека в системі S.W.I.F.T. II

Усі питання, пов'язані з безпекою в системі S.W.I.F.T., умовно можна поділити на такі розділи:

- ☐ фізична безпека;
- ☐ безпека логічного доступу до системи S.W.I.F.T.;
- ☐ забезпечення безпеки повідомлень, переданих і збережених у системі;
- ☐ безпека обміну повідомленнями «користувач – користувач».

Засоби безпеки у системі S.W.I.F.T. II складаються з:

- процедури входу до системи;
- процедури вибору застосунка;
- нумерації повідомлень;
- перевірки помилок передачі;
- криптозахисту повідомлення, що перебуває в мережі S.W.I.F.T.;
- контролю доступу до повідомлень у SAP, регіональних процесорах, комутаційних процесорах, центрах управління системою.

Безпека в системі S.W.I.F.T. II

Відділ головного інспектора системи S.W.I.F.T. (SIO) керує всіма питаннями, пов'язаними із забезпеченням безпеки роботи мережі S.W.I.F.T.

Користувачам рекомендується забезпечувати належну безпеку процедур, здійснюваних у їхніх власних організаціях, наприклад:

- ☐ контроль доступу до терміналів S.W.I.F.T.;
- ☐ керування їхнім підключенням і використанням.
- ☐ і т.п.

Фізична безпека

Фізична безпека здійснюється на основі розмежування та контролю доступу до всіх операційних і адміністративних вузлів S.W.I.F.T. за допомогою використання електронних засобів і засобів виявлення несанкціонованого доступу.

Застосовується також дистанційне керування для вузлів S.W.I.F.T., які управляються автоматично.

Якщо користувач запитує центр про доступ до SAP, то в обов'язковому порядку повинен бути зроблений запит до SIO, і без його санкції нікому не буде надано дозвіл на доступ до SAP.

Безпека логічного доступу до системи S.W.I.F.T.

Користувачі можуть одержати фізичний доступ до системи S.W.I.F.T. тільки через СВТ, що працює з одним або більше користувачами (LT).

Кожному LT призначаються унікальні таблиці безпеки для процедур LOGIN та SELECT (вибір фінансового застосунка FIN), які є послідовностями ключів у табличному вигляді. Кожен ключ у таблиці може бути задіяний тільки один раз і пов'язаний із послідовними номерами процедур, що використовують ці ключі. Зазначені таблиці формуються і відсилаються користувачеві до його підключення до системи S.W.I.F.T. на основі запиту на їх використання.

Нові таблиці безпеки створюються відразу після відсилання чергових таблиць і пересилаються користувачеві тільки у разі необхідності. Користувачі, які активно використовують таблиці безпеки, можуть запросити у відділі головного інспектора таблиці з 2400 ключами замість звичайних таблиць (1200 ключів).

Безпека логічного доступу до системи S.W.I.F.T.

Доступ LT до системи S.W.I.F.T. виконується за допомогою команди LOGIN. До того, як буде відісланий запит LOGIN, користувачеві необхідно ввести ключ запиту та ключ відповіді з таблиці безпеки LOGIN. Мета запиту LOGIN:

- визначити логічний шлях для зв'язку LT із системою;
- обмежити доступ до системи несанкціонованих користувачів;
- дати змогу користувачам перевірити, що вони підключилися до справжньої системи S.W.I.F.T.;
- зазначити розмір вікна, що має бути відкрите для сеансу GPA.

Безпека логічного доступу до системи S.W.I.F.T.

При запиті процедури LOGIN система S.W.I.F.T. виконує таку послідовність дій:

- перевіряє заголовок і текст повідомлення, що відіслане за допомогою процедури LOGIN;
- перевіряє вірогідність кінцевика MAC, який сформований з використанням ключа з таблиці безпеки, але не містить інформації про сам ключ. Якщо підтвердження справжності користувача пройшло успішно, то порядковий номер запиту LOGIN (LSN) порівнюється з очікуваним системою LSN. Якщо LSN з припустимого діапазону, то система перевіряє, що запит LOGIN сформовано після дня, зазначеного в останній команді LOGOUT. Таким чином, враховуються часові рамки для LT, протягом яких від цього LT не будуть прийматися запити. Якщо ж LSN не збігається з очікуваним, то в полі підтвердження справжності системи зазначається наступний очікуваний LSN;
- підтверджує запит LOGIN, повертаючи або позитивне підтвердження LOGIN (LAK), або негативне підтвердження LOGIN (LNK). У підтвердженні є кінцевик MAC, який сформований на ключі відповіді, але не містить інформації про нього та дає змогу користувачеві перевірити автентичність системи;
- записує спробу LOGIN разом із відповіддю системи в передісторію LT.

Безпека логічного доступу до системи S.W.I.F.T.

Спроба зробити запит LOGIN на лінії зв'язку, якою LT уже ввійшов до системи, розглядається як серйозна помилка та ігнорується системою. Доступ до застосунка FIN (з якого відсилаються повідомлення «користувач – користувач» і ряд системних повідомлень) здійснюється за допомогою команди SELECT, що проходить процедуру підтвердження для гарантії такого:

- тільки перевірені користувачі можуть вийти до системи S.W.I.F.T.;
- користувач зв'язався зі справжньою системою S.W.I.F.T. II.

Алгоритм підтвердження автентичності повідомлення формує кінцевик MAC. Це виконується на основі довільного ключа захисту та ключа відповіді, який формується на основі номера запитів LOGIN або SELECT та інших елементів даних (день/час). Цей процес відрізняється від процесу підтвердження автентичності повідомлення «користувач – користувач». Він не потребує обміну ключами автентичності, але замість цього використовуються унікальні таблиці безпеки, створені для кожного користувача.

Безпека логічного доступу до системи S.W.I.F.T.

За винятком довільного ключа захисту та ключа відповіді, що відомі тільки системі S.W.I.F.T. і кінцевому користувачеві, дані для формування MAC надсилаються як частина повідомлень LOGIN та SELECT. У відповідь система S.W.I.F.T. формує новий кінцевик MAC з тим же ключем захисту, але з іншими елементами даних, і включає його до LAK або LNK.

Це дає змогу користувачеві підтвердити автентичність системи S.W.I.F.T. Далі відбувається припинення підключення користувача до системи та формується запит з новим кінцевиком за новим ключем доступу для гарантії того, що сеанс буде відновлений санкціонованим LT з одночасною перевіркою автентичності системи S.W.I.F.T.

Безпека логічного доступу до системи S.W.I.F.T.

Нині у системі S.W.I.F.T. II розроблено та рекомендовано радою директорів для повсюдного використання поліпшену архітектуру системи забезпечення безпеки, що відповідає сучасному рівню розвитку телекомунікаційних технологій і криптографічних методів.

Основою нового підходу стало використання інтелектуальних карт (ICC), зміна алгоритму перевірки автентичності та збільшення довжини двосторонніх ключів, якими обмінюються користувачі. З метою забезпечення безпеки логічного доступу до системи S.W.I.F.T. II у рамках нового підходу було розроблено службу безпечного входу до системи та вибору режиму (SLS), що дає можливість користувачам одержати доступ до послуг системи S.W.I.F.T. за допомогою ICC замість використання паперових таблиць LOGIN та SELECT.

Безпека логічного доступу до системи S.W.I.F.T.

Застосування ІСС потребує використання зчитувача карток (кардридера). Поки пропонується два різні типи зчитувачів карт.

Перший спрощений зчитувач карт (BCR) підтримує тільки службу SLS.

Другий зчитувач карт (SCR) має модуль захисту, в якому, крім функцій кардридера, реалізована також функція модуля апаратного захисту, що виконує генерування ключів і шифрування секретної інформації (застосовується для підтримки як SLS, так і інших служб, створених у рамках нового підходу). Оскільки в модулі захисту SCR повинні зберігатися секретні дані, то він захищений від розкриття – будь-яка спроба дістатися внутрішніх частин пристрою викликає автоматичне знищення секретної інформації, що зберігається в SCR.

Для SCR або BCR передбачено кілька різних варіантів режимів роботи (відключений або підключений до СВТ), широкий перелік варіантів конфігурування цих пристроїв спеціальним персоналом (офіцерами безпеки), а також широкий перелік послуг з навчання персоналу організації.

Служба SLS та операції в рамках цієї служби

Основне призначення служби безпечного входу до системи SLS – заміна паперових таблиць LOGIN/SELECT новим механізмом, здатним генерувати сеансові ключі доступу до системи, які при використанні паперових таблиць доводилося зчитувати операторам СБТ вручну. Необхідно зазначити, що ICC не містить самих ключів доступу, але містить алгоритм, що може генерувати необхідний сеансовий ключ для будь-якого запиту LOGIN/SELECT.

Нині в системі S.W.I.F.T. II цей алгоритм не збігається з алгоритмом генерації для паперових таблиць, тому ключі доступу від ICC відрізняються від своїх еквівалентів у паперових таблицях. Для забезпечення логічного доступу до послуг системи S.W.I.F.T. II необхідно вставити у відповідний спосіб сконфігуровану ICC до зчитувача карт та ввести PIN-код на клавіатурі зчитувача.

Під час вибору функції LOGIN (SELECT) на СБТ необхідні коди автоматично генеруються ICC і передаються у СБТ, до якого підключений зчитувач. Потім СБТ продовжує обробляти запит LOGIN (SELECT) у звичайний спосіб.

Для більшості користувачів зчитувач карт залишатиметься підключеним до СБТ із метою одержання максимальної вигоди від використання служби SLS. Але є можливість використання і непідключеного зчитувача карт (наприклад, для віддалених терміналів або у разі аварії), коли необхідні коди доступу хоча й генеруються в ICC, але тільки відображаються на дисплеї зчитувача карт, а потім вручну вводяться до СБТ.

Забезпечення безпеки повідомлень, переданих і збережених у системі

Система S.W.I.F.T. під час обміну повідомленнями забезпечує:

- безпеку передачі;
- перевірку повідомлень;
- безпеку доставки.

Зокрема, для недопущення несанкціонованого доступу до потоку повідомлень під час їхньої передачі та збереження мережа повинна мати захист від:

- втрати, пошкодження, помилкової доставки або затримки повідомлень;
- помилок під час передачі та збереження;
- втрати конфіденційності;
- внесення до повідомлень помилкових змін.

Забезпечення безпеки повідомлень, переданих і збережених у системі

В усі повідомлення додатків GPA та FIN системи S.W.I.F.T. II додається обов'язковий кінцевик СНК, що містить контрольну суму цього повідомлення, яка перевіряється у вузлах введення/виведення мережі.

Наявність пошкодження повідомлення під час передачі встановлюється у результаті перевірки контрольної суми прийнятого повідомлення (вона є унікальною для кожного повідомлення) з обчисленою контрольною сумою. Якщо наявність пошкодження встановлено (навіть за відсутності зауважень у протоколі перевірок низького рівня), то у відповідь буде передано негативне підтвердження і первинне повідомлення буде надіслано повторно.

Усі вхідні повідомлення перевіряються відповідним регіональним процесором до того, як передати їх комутаційному процесору. Тільки повідомлення, що відповідають стандартам і синтаксису S.W.I.F.T., приймаються до доставки. Результати безперервних перевірок постійно зберігаються. Будь-яка серйозна помилка протоколу призводить за стандартами S.W.I.F.T. до закриття сеансів FIN або GPA.

Забезпечення безпеки повідомлень, переданих і збережених у системі

Після суворих перевірок усіх вхідних потоків повідомлення, що позитивно підтверджені системою S.W.I.F.T., вважаються правильними і транспортуються системою. Обов'язковий кінцевик СНК використовується приймаючим терміналом LT для перевірки того, що жодної помилки не з'явилося під час передачі між вхідним регіональним процесором і кінцевим приймачем.

Для підтвердження правильного прийому кінцевим приймачем інформації в системі S.W.I.F.T. використовується спеціальне повідомлення UAK/UNK.

У системі S.W.I.F.T. повідомлення вважається доставленим тільки тоді, коли термінал-відправник отримає від приймаючого терміналу позитивне підтвердження прийому (UAK). У разі негативного повідомлення (UNK) система S.W.I.F.T. II спробує доставити повідомлення 11 разів, після чого доставка повідомлення припиняється та відправника сповіщають, що повідомлення не може бути доставлене. Для підрахунку спроб кожна наступна спроба доставки після першої міститиме відповідну кількість кінцевиків POM.

Перевірка повідомлень S.W.I.F.T. II гарантує, що повідомлення для підготовки (які мають кінцевик TNG) не можуть бути адресовані вже працюючим приймаючим терміналам, і навпаки, звичайні повідомлення не можуть бути адресовані точкам, що перебувають у стані підготовки до роботи.

Безпека обміну повідомленнями «користувач – користувач»

Під час обміну повідомленнями між користувачами для забезпечення конфіденційності, справжності та цілісності повідомлень система S.W.I.F.T. II рекомендує використовувати алгоритм перевірки автентичності.

Перевірка автентичності є важливою частиною системи забезпечення безпеки S.W.I.F.T. II. Вона ґрунтується на обміні ключами між користувачами та на перевірці відображення автентичності у певних типах повідомлень.

Приймаючий термінал перевіряє текст отриманого повідомлення за допомогою стандартного алгоритму відповідно до погодженого ключа автентичності.

Негативний результат перевірки може відбутися швидше за все через таке:

- помилки передачі;
- неправильний ключ автентичності.

Безпека обміну повідомленнями «користувач – користувач»

Ключ автентичності складається з 32 шістнадцяткових символів, розділених на дві частини по 16 знаків. Він може використовуватися або тільки для передачі, або тільки для прийому, або в обох напрямках. Для формування ключа необхідно дотримуватися таких правил:

- перша та друга половини повинні бути різними;
- у кожній половині будь-який дозволений символ може з'явитися тільки один раз.

Ключі автентичності передаються між кореспондентами поштою. Для забезпечення безпеки ключової інформації всім користувачам системи S.W.I.F.T. II рекомендується підтримувати кореспондентські відносини тільки з відомими користувачами та в організації – ініціаторі обміну вибирати тип ключа автентичності відповідно до вибраної політики безпеки цієї організації.

Безпека обміну повідомленнями «користувач – користувач»

У зв'язку з переходом до нових технологій забезпечення безпеки в системі S.W.I.F.T. II був удосконалений і процес обміну ключами автентичності між користувачами. Результатом стала поява служби обміну двосторонніми ключами (ВКЕ). Призначення ВКЕ – заміна системи ручного обміну двосторонніми ключами підтвердження автентичності між кореспондентами відкритою поштою на систему нових повідомлень S.W.I.F.T. II зі зчитувачем карт із спеціально розробленим модулем захисту.

Нова система дає змогу повністю автоматизувати процес обміну ключами. За новою технологією кожний двосторонній ключ підтвердження автентичності створюється усередині SCR і зашифровується перед передачею у СBT, до якого SCR підключений. Ключі автентичності, якими обмінюються кореспонденти, можуть бути або двоспрямованими (ключ використовується для перевірки автентичності як переданих, так і прийнятих повідомлень окремого кореспондента), або односпрямованими (коли використовуються окремі ключі на прийом і на передачу повідомлень).

Безпека обміну повідомленнями «користувач – користувач»


Служба ВКЕ базується на стандарті ISO з обміну ключами (ISO 11166 Banking Key Management by Means of Asymmetric Algorithms). Цим стандартом передбачено використання асиметричних алгоритмів для шифрування та цифрового підпису двосторонніх ключів, якими обмінюються кореспонденти.

Спеціально для забезпечення розподілу відкритих ключів у системі S.W.I.F.T. II був створений центр управління безпекою (SMC), у складі якого працює центр сертифікації ключів, що видає сертифікати відкритих ключів користувачам системи S.W.I.F.T. II.

Безпека обміну повідомленнями «користувач – користувач»

Процедура обміну двосторонніми ключами автентичності у S.W.I.F.T. містить у собі обмін чотирма спеціальними повідомленнями між ініціатором обміну та одержувачем. Перші два повідомлення необхідні тільки для встановлення сеансу обміну двосторонніми ключами. У третьому повідомленні ініціатор обміну надсилає ключ, створений і зашифрований усередині SCR, використовуючи відкритий ключ одержувача. В свою чергу, SCR створює цифровий підпис ініціатора обміну ключами. Після одержання третього повідомлення одержувач перевіряє цифровий підпис. Якщо він правильний, то ініціатору обміну відсилається підтвердження, а ключ заноситься до файлу двосторонніх ключів. У четвертому повідомленні одержувач відсилає ключ ініціатору обміну за аналогічною процедурою.

Безпосередньо після обміну новий ключ стає майбутнім ключем для цих кореспондентів і використовуватиметься для перевірки фінансових повідомлень, починаючи із взаємно погоджених дати та часу. При використанні ключів прийому/передачі кожний кореспондент є ініціатором обміну для свого ключа передачі.

A blue key is positioned diagonally across the frame. The background is a light blue gradient with a pattern of binary code (0s and 1s) in a darker blue, creating a digital or technological theme. The key has a circular head and a notched bit.

Дякую за увагу
Лекцію закінчено