Розділ 6

КРИПТОГРАФІЧНІ ПРОТОКОЛИ АВТЕНТИФІКАЦІЇ ТА ВСТАНОВЛЕННЯ КЛЮЧІВ НА ОСНОВІ ЕЦП

Одним із найважливіших і розповсюджених методів (механізмів) захисту інформації є використання протоколів, зокрема криптографічних протоколів. Вони є основними механізмами при автентифікації, управлінні та сертифікації ключів, а також при безпосередньому захисті інформації та ресурсів. Чільне місце серед них посідають криптографічні протоколи, у яких або складовим елементом, або основним механізмом забезпечення неспростовності, цілісності та справжності є застосування ЕЦП. У подальшому під протоколом цифрового підпису [32, 210] будемо розуміти алгоритм дій двох або більше суб'єктів з доведенням того, що деяка інформація є цілісною, справжньою та належить одному суб'єктові – учаснику протоколу.

Метою цього розділу є розгляд і аналіз сучасних криптографічних механізмів та на їх основі – криптографічних протоколів з використанням ЕЦП, що застосовуються як для безпосереднього захисту інформації, так і для управління та сертифікації ключів, розподілу таємниці тощо.

6.1. ВИЗНАЧЕННЯ ТА КЛАСИФІКАЦІЯ КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ

Існують різні погляди на криптографічні протоколи щодо їх сутності, застосування, властивостей тощо. У найбільш спрощеному вигляді на практиці криптографічний протокол – це визначена послідовність дій учасників обміну інформацією, у якій хоча б одна дія є криптографічним перетворенням повідомлень. У найбільш узагальненому вигляді криптографічний протокол – це розподілений криптографічний алгоритм дії або взаємодії $n \geq 2$ об'єктів та/або суб'єктів інформаційної або інформаційно-телекомунікаційної системи. Тобто сукупність криптографічних алгоритмів, які виконуються за допомогою криптографічних перетворень обробки інформації (у тому числі ключових даних) з метою забезпечення конфіденційності, цілісності, справжності, доступності, спостережливості, неспростовності тощо як з кожним із них окремо, так і при обміні інформацією між собою з метою узгодження, встановлення, передавання й підтвердження ключових даних (ключової інформації) [7, 22, 56, 210], причому при обробці та обміні інформацією вони використовують погоджені формати даних, повідомлень, команд, програмного забезпечення, погоджені специфікації синхронізації різних дій тощо.

До криптографічних протоколів пред'являється ряд складних вимог щодо забезпечення необхідного рівня їх безпеки. Останні дослідження підтвердили той факт, що для надійної автентифікації необхідно використовувати механізми автентифікації, перш за все з використання ЕЦП. Вони також повністю або як елементи можуть входити в криптографічні протоколи автентифікації. Тому криптографічні протоколи на основі ЕЦП, у тому числі автентифікації, є важливою складовою криптографічних протоколів взагалі.

Криптографічні протоколи, у тому числі автентифікації, можна класифікувати залежно від їхнього функціонального призначення, застосовуваного математичного апарату, кількості раундів при взаємодії, можливостей застосування протоколу без з'єднання під час виконання протоколу та багатьох інших властивостей. Протоколи можуть бути інтерактивними або неінтерактивними. *Інтерактивним протоколом* називається протокол, під час виконання якого між суб'єктами, що виконують протокол, відбувається обмін даними. *Неінтерактивний протокол* – це протокол, під час виконання якого між суб'єктами, виконуючими протокол, не здійснюється обмін даними. У свою чергу інтерактивні протоколи можна класифікувати за кількістю раундів (сеансів зв'язку) на одно- та багатораундові. *Одноразундові протоколи* вимагають не більше одного сеансу передачі даних. *Багатораундові протоколи* – це такі протоколи, які для виконання всіх встановлених протоколом дій вимагають 2 та більше раундів. У той же час на практиці виникають ситуації, коли обмін під час з'єднання не може бути здійснений або взагалі не бажаний.

Початкову класифікацію можна виконати за функціональним призначенням. У цьому випадку розрізняють: криптографічні протоколи автентифікації, протокол цифрового підпису, встановлення ключів, узгодження ключів, вироблення спільної таємниці, розділення таємниці, передавання та транспортування ключів, підтвердження ключів, спрямованого шифрування, ідентифікації тощо. Як правило, указані криптографічні протоколи виконуються на основі застосування симетричних та асиметричних криптоперетворень. ЕЦП є одним із важливих криптографічних перетворень, що застосовуються для надання таких послуг, як цілісність, справжність (автентичність), підтвердження авторства, неспростовність тощо як при виконанні протоколів, так і при обміні повідомленнями.

Протокол ідентифікації [210] – алгоритм спільних дій двох суб'єктів з доведення особистості одного із суб'єктів-учасників протоколу.

Протокол цифрового підпису [32, 34, 210] – алгоритм дій двох або більше суб'єктів з доведення того, що деяка інформація є цілісною, справжньою та належить одному суб'єктові – учасникові протоколу.

Дуже важливими характеристиками криптографічного протоколу є автентичність суб'єктів, які взаємодіють, автентичність ключів і криптографічна живучість ключів [21, 37, 210]. Тому розглянемо основні поняття та визначення щодо криптографічних протоколів автентифікації.

Автентифікація – встановлення достовірності твердження, що об'єкт [суб'єкт] має очікувані властивості. Як правило, достовірність твердження встановлюється з деякою ймовірністю. Тому має право на існування й таке визначення: ***автентифікація об'єкта (суб'єкта)*** *(en entity authentication)* –

це підтвердження з заданою ймовірністю того, що об'єкт (суб'єкт) є тим, за кого він себе видає.

З метою однозначного трактування, ґрунтуючись на ISO/IEC 7498, уведемо також поняття криптографічного механізму.

Криптографічний механізм захисту – конкретний процес, криптографічний протокол або криптографічний алгоритм, що використовується для реалізації визначених послуг та/або функцій криптографічного захисту інформації та інформаційних ресурсів.

Наведемо також деякі поняття та визначення відносно складових частин механізмів автентифікації, які будуть потрібні в подальшому.

Автентифіковані ідентифікаційні дані (*Authenticated identity*) – розпізнавальний ідентифікатор комітента, що підтверджений з використанням механізму автентифікації.

Метод асиметричної автентифікації (*Asymetric authentication methiod*) – метод автентифікації, у якому два об'єкти не розподіляють між собою всю інформацію автентифікації.

Сертифікат автентифікації (*authentication certificate*) – сертифікат безпеки, гарантування справжності якого забезпечується уповноваженим на автентифікацію і який можна використовувати для підтвердження ідентифікаційних даних користувача.

Обмін при автентифікації (*authentication exchange*) – послідовність одного чи декількох передавань інформації автентифікації, якою обмінюються для того, щоб здійснити автентифікацію.

Інформація автентифікації (*authentification information*) – інформація, яку використовують з метою проходження автентифікації.

Ініціатор автентифікації (*authentication initiator*) – об'єкт, що розпочинає обмін при автентифікації.

Заявлена інформація автентифікації (*claim authentication information*) – інформація, яку використовує пред'явник для генерування інформації автентифікації обміну при автентифікації комітента.

Пред'явник (*claimant*) – об'єкт, який є комітентом або його представляє з метою здійснення автентифікації. До пред'явників належать також функції, що необхідні для залучення до обмінів при автентифікації від імені комітента.

Розпізнавальний ідентифікатор (*distinguishable identifier*) – дані, згідно з якими однозначно розпізнають об'єкт у процесі проходження автентифікації.

Обмінна інформація автентифікації (*exchange authentication information*) – інформація, якою обмінюються пред'явник і перевірник під час процесу проходження автентифікації комітента.

Автономний сертифікат автентифікації (*Off-line authentication certificate*) – сертифікат автентифікації, який зв'язує розпізнавальний ідентифікатор з перевірочною інформацією автентифікації, що доступна всім об'єктам.

Інтерактивний сертифікат автентифікації (*on-line autentication certificate*) – сертифікат автентифікації, що використовується в обміні при автентифікації й одержаний безпосередньо пред'явником від уповноваженого, який надає гарантії щодо справжності сертифіката.

Комітент (*principal*) – суб'єкт, ідентифікаційні дані якого можна підтвердити. У тлумачному словнику *комітент* – юридична або фізична особа, яка доручає комісіонерові здійснити за винагороду певну операцію.

Змінний у часі параметр (*time variant parameter*) – елемент даних, який використовує об'єкт для перевірки того, що повідомлення не відтворене повторно.

Унікальне число (*unique number*) – змінний у часі параметр, який генерує пред'явник.

Перевірочна інформація автентифікації (*verification authentication information*) – інформація, яку використовує перевірник для перевірки ідентифікаційних даних, що заявлені за допомогою обмінної інформації автентифікації.

Перевірник (*verifier*) – представник об'єкта або сам об'єкт, якому потрібні автентифіковані ідентифікаційні дані. До перевірників належать також функції, необхідні для залучення в обміни при автентифікації.

Явна автентифікація ключа суб'єктом B суб'єкта A (*en explicit key authentication from A to B*) – гарантія для суб'єкта *B* того, що суб'єкт *A* є єдиним іншим суб'єктом, який має правильний ключ.

Неявна автентифікація ключа суб'єктом B суб'єкта A (*en implicit key authentication from A to B*) – гарантія для суб'єкта *B* того, що суб'єкт *A* є єдиним іншим суб'єктом, який може володіти правильним ключем.

Узгодження ключів (*en key agreement*) – процес встановлення розділюваного таємного ключа між суб'єктами таким чином, щоб жоден із суб'єктів практично (з наперед заданою ймовірністю) не міг наперед визначити значення цього ключа (розділюваного таємного ключа).

Підтвердження ключа суб'єкта B суб'єктом A (*en key confirmation from A to B*) – гарантія для суб'єкта *B* того, що суб'єкт *A* має правильний ключ.

Встановлення ключа (*en key establishment*) – процес забезпечення доступності розділюваного таємного ключа для одного чи багатьох суб'єктів (об'єктів). Встановлення ключів включає узгодження ключів або передавання ключів.

Маркер ключа (*en key token*) – повідомлення з управління ключами, що відсилається від одного суб'єкта до іншого під час виконання протоколу управління ключами.

Передавання ключа (*en key transport*) – процес передавання ключа від одного суб'єкта до іншого з належним рівнем захищеності.

Взаємна автентифікація суб'єктів (*об'єктів*) (*en mutual entity authentication*) – така автентифікація суб'єктів (об'єктів), за якої обом суб'єктам (об'єктам) забезпечується гарантія справжності одне одного.

Порядковий номер (*en sequence number*) – змінюваний з часом параметр, значення якого обирається з визначеної послідовності і не повторюється у наперед визначеному періоді часу.

Позначка часу (*en time stamp*) – параметр, що змінюється з часом і позначає моменти часу відносно загально прийнятого в системі еталона часу.

Змінюваний з часом параметр (*en time variant parameter*) – елементи даних, таких як випадкове число, порядковий номер чи позначка часу, що використовуються суб'єктом (об'єктом) для перевіряння того, що повідомлення, яке приймається, не є повтором раніше прийнятого.

Третя довірча сторона (*en trusted third party*) – орган з безпеки інформації або його агент, якому інші суб'єкти довіряють щодо діяльності, пов'язаної з безпекою інформації.

Протокол вироблення спільної таємниці (ключа) [22, 37] – це алгоритм спільних дій двох суб'єктів з використанням передачі даних по відкритому каналу з метою вироблення послідовності символів (спільної таємниці), які відомі тільки суб'єктам, що виконували протокол.

Протокол розділення таємниці [22, 37, 210] – це алгоритм дій не менше ніж трьох суб'єктів, один із яких виконує певні дії з метою розподілу між іншими суб'єктами інформації, необхідної для відновлення секретних даних. При цьому інформація розподіляється таким чином, щоб секретні дані надалі могли бути відновлені певним компетентним набором учасників протоколу (не обов'язково всіма суб'єктами).

Протокол спрямованого шифрування [210] – це алгоритм спільних дій двох суб'єктів, що виконується з метою генерації спільних секретних даних і подальшого спрямованого шифрування інформації для передачі по відкритому каналу. У більшості випадків початковим етапом у протоколах такого типу є протоколи формування спільної таємниці або їхньої модифікації.

Статичний ключ – це спільний ключ (секрет), що встановлюється однаковим при кожному виконанні криптографічного протоколу встановлення ключів.

Протокол встановлення динамічних ключів – це протокол при виконанні якого ключ, що встановлюється об'єктами, змінюється при кожному новому встановленні ключів. Іншими словами, протоколи встановлення динамічних ключів встановлюють сеансові ключі. Такі протоколи є стійкими до вторгнень активних порушників з відомим ключем.

Однією з основних властивостей протоколу встановлення ключів є його безпека. По суті, безпека встановлення ключів характеризує протистояння можливості обчислення ключа несанкціонованими об'єктами.

У найбільш узагальненому вигляді автентифікація забезпечує гарантії заявлених ідентифікаційний даних об'єкта. Автентифікація може розглядатися тільки в контексті взаємовідносин між комітентом і об'єктом, який перевіряє, тобто перевірником. Автентифікація, залежно від особливості її здійснення, може бути зведена до двох варіантів:

1) комітента представляє пред'явник, який має особисті комунікаційні взаємовідносини з тим, хто перевіряє – перевірником (об'єктна автентифікація – entity authentication);

2) комітент є ресурсом елемента даних, що доступний перевірнику (оригінальна ідентифікація даних – data origin authentication).

Автентифікація об'єкта забезпечує підтвердження ідентифікаційних даних комітента в рамках комунікаційних взаємовідносин. Автентифіковані дані комітента підтверджуються тільки тоді, коли надається такий сервіс.

Автентифікація походження даних забезпечує підтвердження ідентифікаційних даних комітента, що несе відповідальність за визначений елемент даних.

У подальшому викладення матеріалу пов'язане із сутністю оцінок якості автентифікації та механізмами (протоколами) автентифікації на основі ЕЦП.

6.2. ОСНОВНІ КОНЦЕПЦІЇ АВТЕНТИФІКАЦІЇ НА ОСНОВІ ЕЦП

Основні концепції автентифікації розглянемо, спираючись на добре апробовану сукупність міжнародних стандартів ISO/IEC 10181 [210], ISO/IEC 9797-1, ISO/IEC 9797-2 [211, 212], ISO/IEC 9798-1(2,4,5,6), гармонізовані національні стандарти ДСТУ ISO/IEC 15946-3 [36], ДСТУ ISO/IEC 11770-3 [22], ДСТУ ISO/IEC 9798-3 [213], а також нові їх версії, які, ми сподіваємося, найближчим часом будуть гармонізовані в Україні.

6.2.1. Ідентифікація та автентифікація

Комітентом є об'єкт, ідентифікаційні дані якого можна автентифікувати; при цьому він може мати один чи декілька розпізнавальних ідентифікаторів, що асоційовані з ним. Ідентифікаційні дані перевіряються за допомогою послуг автентифікації, і після проходження автентифікації мають назву *ідентифікаційних даних, що автентифіковані.*

Вимогою до розпізнавальних ідентифікаторів є визначеність щодо даного домену безпеки. Існує дві основні ознаки, за якими розпізнавальні ідентифікатори відрізняють конкретного комітента від інших учасників домену:

1) на основі членства в групі об'єктів, тобто з груповим рівнем модульності, у якому об'єкти розглядаються еквівалентно цілям автентифікації (у даному випадку ціла група розглядається як один комітент, що має один розпізнавальний ідентифікатор);

2) на основі індивідуального членства, коли ідентифікується один, і тільки один об'єкт.

Якщо автентифікація виконується між різними доменами безпеки, використання розпізнавального ідентифікатора не достатньо для того, щоб однозначно ідентифікувати об'єкт. Це пов'язане з тим, що різні уповноважені доменів безпеки можуть використовувати однакові розпізнавальні ідентифікатори. У цьому випадку розпізнавальні ідентифікатори необхідно використовувати разом з ідентифікатором домену безпеки.

6.2.2. Об'єкти автентифікації

Необхідно розглядати три об'єкти автентифікації – об'єкт «пред'явник», об'єкт «перевірник» та об'єкт «третя довірча сторона» (ТДС).

Об'єкт «пред'явник» – використовується для опису, тобто представлення характеристик об'єкта, який або є комітентом або його представляє з метою проходження автентифікації. Як зазначалося раніше, до пред'явників належать також функції, необхідні для залучення в обміни при автентифікації від імені комітента.

Об'єкт «перевірник» – використовується для опису, тобто представлення, характеристик представника об'єкта або об'єкта, якому необхідні ідентифікаційні дані, що автентифіковані. У випадку залучення об'єкта до взаємної автентифікації, він може виконувати дві ролі – пред'явника та перевірника.

Об'єкт «третя довірча сторона» – використовується для опису уповноваженого безпеки або його агента, якому довіряють інші об'єкти щодо діяльності, пов'язаної з безпекою. Для проходження автентифікації необхідна повна довіра третій довірчій стороні як з боку пред'явника, так і з боку перевірника.

6.2.3. Інформація автентифікації

Інформацію автентифікації можна розділити на такі види:

1) інформація автентифікації, що використовується для здійснення обміну (в подальшому ІА обміну);

2) заявлена інформація автентифікації (заявлена ІА);

3) інформація автентифікації для здійснення перевірки (ІА перевірки).

Загальна модель використання інформації автентифікації в процесі автентифікації показана на рис. 6.1. Розглянемо основні зв'язки, які виникають в процесі автентифікації. Для опису послідовності одного чи декількох передавань обмінної інформації автентифікації з метою проходження автентифікації використовується *поняття «елемент обміну»*.

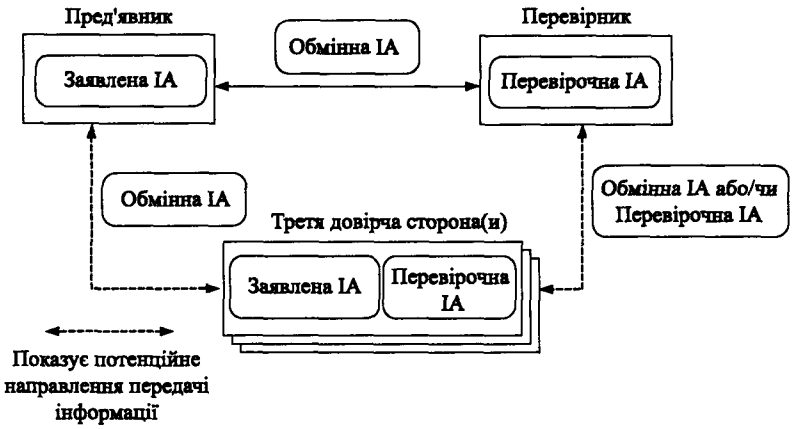

Рис. 6.1. Загальна модель використання інформації в процесі автентифікації

У ряді випадків для генерування обмінної ІА пред'явнику необхідно взаємодіяти з третьою довірчою стороною. Перевірник для перевірки обмінної ІА також у деяких випадках повинен взаємодіяти з третьою довірчою стороною. За таких умов третя довірча сторона володіє перевірочною ІА, що зв'язана з пред'явником.

Третя довірча сторона (ТДС) може залучатися до передачі обмінної ІА, при цьому для автентифікації третьої довірчої сторони об'єктам необхідно володіти інформацією автентифікації відносно ТДС.

6.2.4. Основні положення надання послуг автентифікації

Загрози автентифікації

Основною задачею автентифікації є надання гарантій справжності ідентифікаційних даних комітента. Механізми автентифікації повинні виключати можливість реалізації загроз типу «Маскарад» і «Повтор».

Загроза типу «Маскарад» полягає в обмані одного об'єкта іншим об'єктом. Це означає, що один об'єкт особливим чином впливає на інший об'єкт, наприклад, використовуючи джерело даних або використовуючи інші інформаційні взаємовідносини. Цей вид загроз включає загрози типу «Повтор», заміну та компрометацію

заявленої інформації автентифікації. Загроза типу «Маскарад» реалізується в контексті активності джерела даних, комунікаційних взаємозв'язків тощо, що ініціюються або пред'явником, або перевірником. Для захисту проти загроз типу «Маскарад» краще використовувати послугу надання цілісності з використанням для обміну при автентифікації відповідних елементів даних. Для протистояння загрозам, що належать до такого типу, в процесі автентифікації повинні використовуватися спеціальні дані, що пов'язані з деяким механізмом реалізації послуги цілісності, наприклад, ЕЦП чи кодом автентифікації.

Загроза типу «Повтор» полягає у повторі обмінної інформації автентифікації, що була передана раніше. Зазвичай її використовують у комбінації з іншими атаками, наприклад такими, як атака типу «Модифікація». Не всі механізми автентифікації однаково протистоять атакам типу «Повтор». Атака типу «Повтор» може бути загрозою й для інших послуг безпеки, наприклад неспростовності й автентичності. Механізми автентифікації на основі ЕЦП можна використовувати для протистояння атакам типу «Повтор», оскільки ЕЦП забезпечує послугу неспростовності пред'явника.

Направлена автентифікація (за дорученням)

У деяких випадках комітент може бути представлений опосередковано. За таких умов необхідно формувати його представлення, або перед формуванням представлення комітент повинен бути автентифікований. Тому, коли дія відбувається від імені комітента, замість використання ідентифікаційних даних комітента необхідно автентифікувати того, хто його представляє. Пов'язано це з тим, що представлення діє так, начебто це комітент, при цьому дії від імені комітента можуть продовжуватись у системі без необхідності прямого залучення комітента. Коли комітентом є людина, тоді можна використовувати механізми, що обмежують тривалість дії представлення до тих пір, поки користувач фізично присутній у визначеному місті.

При діях від імені комітента необхідно мати доступ до іншої системи, яка забезпечує вироблення особистого представлення комітенту згідно з механізмом автентифікації. На вироблення цього представлення посилаються як на направлену автентифікацію (за дорученням). Здійснення направленої автентифікації в такий спосіб може бути досягнуто за рахунок реалізації відповідної політики безпеки.

Однобічна та взаємна автентифікація

Два взаємодіючих об'єкти чи суб'єкти можуть реалізовувати механізми однобічної або двосторонньої автентифікації. Однобічна автентифікація надає гарантії щодо автентифікації й відповідно ідентифікації тільки одного комітента. Механізм взаємної автентифікації надає гарантії щодо автентифікації й відповідно ідентифікації обох комітентів. Автентифікація об'єктів може бути як взаємною, так і однобічною, але автентифікація джерела даних може бути тільки однобічною.

Ініціювання обміну при автентифікації

Обмін при автентифікації може ініціюватися або пред'явником, або перевірником. Об'єкт, який розпочинає обмін, має назву *ініціатор автентифікації*. Кожен із об'єктів або суб'єктів може бути як пред'явником, так перевірником, у тому числі й одночасно.

Відкликання інформації автентифікації

За необхідності інформація автентифікації може бути відкликана, тобто заборонена до використання. Відкликання інформації автентифікації стосується довгострокового анулювання перевірочної інформації автентифікації.

Відкликання інформації автентифікації може здійснюватись у визначених політикою безпеки випадках. Прийняття рішення щодо відкликання інформації автентифікації може базуватися на визначенні подій, які є порушенням визначеної політики безпеки, зміні політики або з інших причин. При відкликанні інформації автентифікації може здійснюватись або не здійснюватись відкликання (заборона) існуючого доступу, або інші наслідки згідно діючої політики безпеки. Додатково при відкликанні інформації автентифікації можуть здійснюватись також такі події:

– запис усіх або тільки обмежених подій у журнал аудиту;

– локальне повідомлення, наприклад адміністратора, про подію;

– віддалене повідомлення про подію відповідальних за реалізацію політики безпеки;

– розрив або блокування комунікаційних відносин.

Виконання специфічних дій унаслідок порушень залежить від діючих політик безпеки на різних етапах взаємодії та інших факторів, пов'язаних зі статусом комунікаційних відносин, наприклад, чи відбулося відновлення, коли комітента допустили до системи та змінили його активний статус тощо.

Гарантія безперервності автентифікації

Автентифікація об'єкта надає гарантії ідентифікації об'єкта чи суб'єкта тільки в поточний момент часу. Одним із шляхів одержання гарантій безперервності автентифікації є зв'язування послуги автентифікації з послугою цілісності даних, перше за все на основі використання ЕЦП. Послуги автентифікації та забезпечення цілісності пов'язані між собою тільки тоді, коли комітент постійно автентифікується, використовуючи послугу автентифікації, а подальші відправлені від його імені дані передаються разом з обмінною інформацією автентифікації з використанням послуги забезпечення цілісності, наприклад, на основі застосування ЕЦП. За такої умови гарантується неможливість подальшої зміни інформації будь-яким іншим об'єктом. Вона з гарантією надходить тільки від комітента, що постійно здійснює автентифікацію із застосуванням указаного вище механізму. Щодо підписаної інформації може бути забезпечена цілісність на всіх етапах життєвого циклу, наприклад, при проходженні інформації від комітента до перевірника. За таких умов здійснити атаку типу «Маскарад» можна за умови, якщо комітент відмінний від автентифікованого та може формувати деяку специфічну інформацію, наприклад, володіє особистим ключем ЕЦП.

Іншим шляхом одержання гарантій того, що той самий зовнішній об'єкт все ще існує, є виконання подальших обмінів при автентифікації із забезпеченням цілісності. Однак за вказаних умов не забезпечується запобігання втручання в інтервалах між обмінами. Таким чином, неможливо одержання повних гарантій нерозривності автентифікації. Наприклад, можлива така атака: порушник протягом запиту на проведення подальшої автентифікації дозволяє справжньому

об'єкту чи суб'єкту здійснювати автентифікацію. Але після завершення дій порушник знову може робити спроби здійснювати автентифікацію від імені попередньої сторони.

Якщо механізм забезпечення цілісності потребує застосування ключа, то цей ключ можна виробляти з параметрів, визначених під час обміну при автентифікації. Узгоджений або встановлений таким чином ключ зв'язаний з автентифікованим комітентом, тому при використанні його в механізмі забезпечення цілісності, по суті, поєднуються дві послуги – справжність і цілісність.

Механізм вироблення ключа для послуги забезпечення цілісності можна розглядати через частину параметрів, яка визначає методи й алгоритми автентифікації та повинна використовуватися протягом усього обміну при автентифікації.

Розподіл компонент автентифікації через складені домени

Виникає ряд завдань, коли між доменами безпеки повинне здійснюватись входження у взаємовідносини таким чином, щоб пред'явник одного домену міг здійснювати автентифікацію з перевірником іншого домену. Такі домени безпеки, що називаються *складеними*, можуть включати:

– домен безпеки, де знаходиться ініціатор;

– домен безпеки, де знаходиться перевірник;

– домен безпеки, у якому знаходиться третя довірча сторона.

Наведені домени не повинні бути різними за можливостями та специфікаціями.

Об'єкти, що використовуються при автентифікації

Взагалі кожен метод автентифікації залежить від припущень або допущень, пов'язаних з одним або декількома комітентами.

Дії комітента можуть спиратися:

– на певне знання, наприклад знання пароля або ключа;

– на певну власність, наприклад електронний засіб;

– на певну незмінну характеристику, наприклад, біометричний ідентифікатор;

– на визнання того, що третя сторона встановила автентифікацію;

– на контекст, наприклад, адресу комітента.

Кожен з розглянутих варіантів має притаманні йому недоліки або слабкі місця. Наприклад, при автентифікації деякої власності скоріш за все автентифікується об'єкт власності, ніж його власник. У деяких випадках уразливості можна перекрити, застосовуючи метод розподілу таємниці, комбінацію декількох варіантів тощо. Наприклад, коли використовується електронний ключ (як особиста власність), уразливість можна перекрити, використавши особистий ключ ЕЦП.

Виконання автентифікації третьою довірчою стороною може бути здійснене двома способами:

1) при ідентифікації третя сторона може сама вимагати, щоб з нею виконали автентифікацію;

2) третя сторона може здійснювати автентифікацію, використовуючи інший об'єкт.

6.2.5. Фази автентифікації. Сутність фаз автентифікації

Процес автентифікації складається з таких фаз (рис. 6.2).

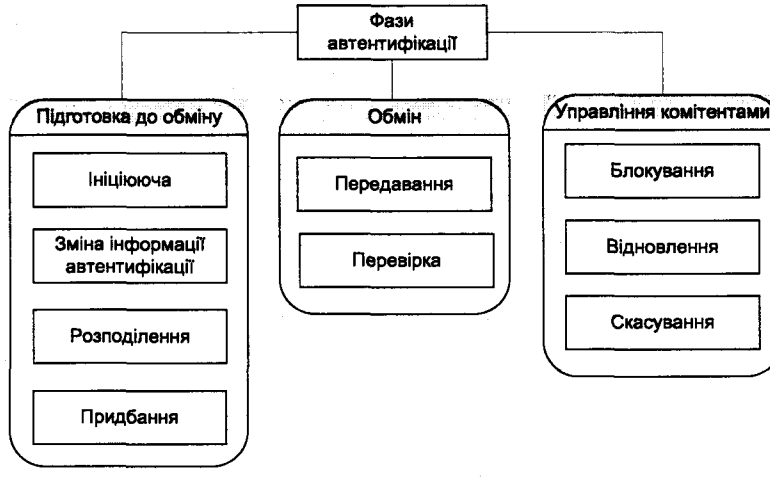

Рис. 6.2. Фази автентифікації

Необхідно зважати на те, що використання всіх фаз окремо в часі є необов'язковим, саме використання може перекриватися (наприклад, виконуватися одночасно, а послідовність фаз, поданих на рис. 6.2, може застосовуватись залежно від конкретного механізму.

На рис. 6.2 визначення фаз подано в такому розумінні.

Ініціююча фаза. На цій фазі повинна бути заявлена та перевірочна інформація автентифікації.

Змінна інформації автентифікації. Це заявлена та перевірочна інформація автентифікації, яку комітент або менеджер представляє для її зміни.

Розподілення. На цій фазі перевірочна інформація автентифікації об'єкта (наприклад, пред'явника або перевірника) розподіляється для використання при перевірці обмінної інформації автентифікації. Так, в автономному режимі роботи об'єкти – користувачі інфраструктури відкритих ключів, можуть одержувати сертифікати автентифікації, списки відкликаних сертифікатів та списки відкликаних уповноважених. Причому фаза розподілення може виконуватись перед передаванням, протягом або після фази передавання.

Перевірка. На цій фазі пред'явник або перевірник можуть одержувати інформацію, потрібну для генерування особливої обмінної інформації автентифікації для потреби автентифікації. Причому можуть реалізовуватись різні процедури перевірки обмінної інформації автентифікації, перш за все за рахунок взаємодії з третьою довірчою стороною або за рахунок обміну повідомленнями між сторонами, що здійснюють автентифікацію.

Наприклад, при використанні центру розподілення ключів в інтерактивному режимі пред'явник або перевірник можуть одержувати від центру розподілення ключів для автентифікації з іншим об'єктом таку інформацію, як сертифікат автентифікації.

Передавання. Це фаза передавання обмінної інформації автентифікації між пред'явником та перевірником.

Перевіряння. На цій фазі перевіряється на відповідність перевірочній інформації автентифікації обмінна інформація автентифікації. На цій фазі об'єкт, який неспроможний перевірити обмінну інформацію автентифікації самостійно, може взаємодіяти з третьою довірчою стороною, що виконує перевірку обмінної інформації автентифікації. У цьому випадку третя довірча сторона буде повертати позитивну або негативну відповідь.

Блокування. Це фаза встановлення тимчасового стану неможливості автентифікації для комітента, який раніше, можливо, був автентифікований.

Відновлення. Це фаза припинення стану блокування комітента.

Скасування. Фаза видалення комітента з переліку санкціонованих комітентів.

Залучення третьої довірчої сторони

Для здійснення автентифікації може залучатися або не залучатися ТДС. Розрізнюють такі типи автентифікації:

- автентифікація без залучення третьої довірчої сторони;
- автентифікація із залученням третьої довірчої сторони;
- автентифікація за допомогою посередника;
- інтерактивна автентифікація;
- автономна автентифікація;
- автентифікація, коли пред'явник довіряє перевірнику.

Автентифікація без залучення ТДС

При автентифікації без залучення третьої довірчої сторони ні пред'явнику, ні перевірнику будь-якою іншою стороною не надається підтримка в генеруванні та перевірянні обмінної інформації автентифікації (рис. 6.3). У цьому випадку перевірочна інформація автентифікації комітента повинна бути вже встановлена перевірником.

Основними недоліками цього методу є:

1) обмеження кількості можливих партнерів взаємовідносин;

2) обмежене використання в широкомасштабних середовищах;

3) у найгіршому випадку перевірнику потрібно мати перевірочну інформацію автентифікації для всіх комітентів домену безпеки, тому об'єм загальної інформації зростає, як квадрат числа залучених об'єктів.

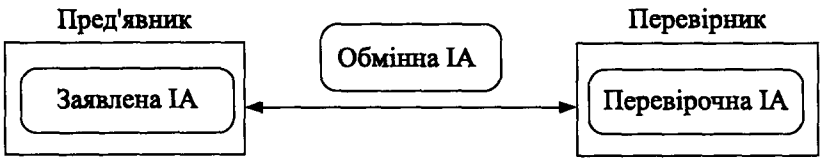

Рис. 6.3. Автентифікація без залучення ТДС

Автентифікація із залученням ТДС

Основною відмінністю при автентифікації із залученням третьої довірчої сторони є можливість одержання перевірочної інформації автентифікації за рахунок взаємодії з третіми довірчими сторонами за умови надання гарантії цілісності цієї інформації. Також необхідна підтримка конфіденційності заявленої інформації автентифікації третьої довірчої сторони, причому перевірочна ІА може виводитись із заявленої ІА.

У процесі автентифікації може залучатись одна або послідовність (ланцюг) третіх довірчих сторін.

Основною перевагою залучення третіх довірчих сторін є забезпечення проведення автентифікації між великою множиною об'єктів, кожен з яких підтримує інформацію тільки про обмежену кількість об'єктів, але не про всіх інших. Тому загальна інформація може зростати лінійно зі збільшенням числа залучених об'єктів.

Автентифікація за допомогою ТДС як посередника

В автентифікації за допомогою посередника комітент автентифікується третьою довірчою стороною, що виступає в ролі посередника, а потім ручається за ідентифікаційні дані в підпослідовності обмінної ІА (рис. 6.4).

Основні вимоги при автентифікації за допомогою ТДС:

1) основною вимогою щодо перевірника є необхідність довіри посереднику мати права вже автентифікованого комітента;

2) необхідно також гарантувати ідентифікацію посередника перевірником шляхом автентифікації.

Для запобігання нерегламентованим спробам автентифікації ТДС повинна контролювати статус можливості автентифікації. Якщо пред'явнику необхідно відкликати інформацію автентифікації, то посередник може змінити статус пред'явника й відхилити наступні спроби автентифікації.

Даний тип автентифікації припускає залучення ланцюжка довірчих посередників із забезпеченням гарантій щодо них. Залежно від діючої політики безпеки за визначення справжності послідовності посередників відповідальність несе або перевірник, або ТДС.

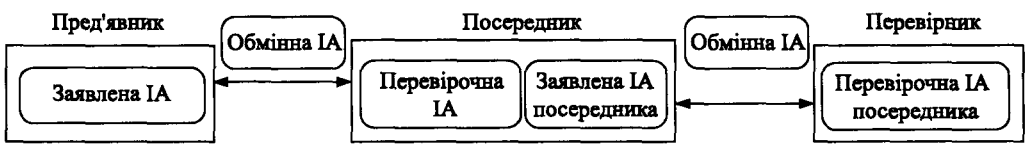

Рис. 6.4. Автентифікація за допомогою ТДС як посередника

Інтерактивна автентифікація

При інтерактивній автентифікації одна або декілька третіх довірчих сторін беруть активну участь в обміні інформацією. На відміну від автентифікації з посередником, при інтерактивній автентифікації між пред'явником і перевірником обмінна ІА не проходить безпосередньо через

ТДС. ТДС використовується пред'явником для генерування обмінної ІА, а перевірником – для підтримки його в перевірці обмінної ІА. ТДС в інтерактивній автентифікації може генерувати сертифікати в інтерактивному режимі (рис. 6.5).

Вимоги до типу інтерактивної автентифікації:

1) повинна існувати послідовність третіх довірчих сторін, які залучені в генерування обмінної ІА між перевірником і ТДС, що можуть підтвердити заявлену ІА комітента;

2) у найпростішому випадку для взаємодії безпосередньо з пред'явником або перевірником необхідна тільки одна третя довірча сторона. Але їх можна розширити до послідовності третіх довірчих сторін для безпосередньої або опосередкованої взаємодії з пред'явником чи перевірником.

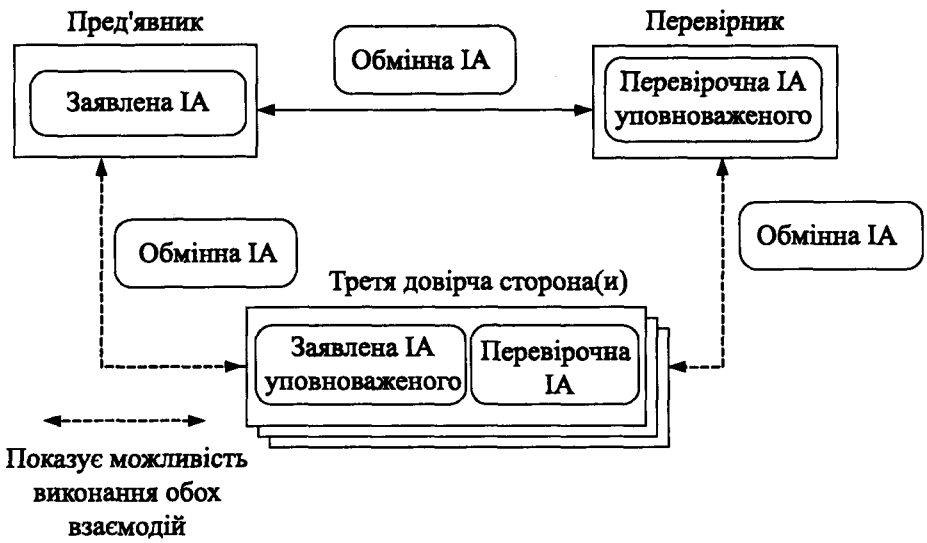

Рис. 6.5. Інтерактивна автентифікація

Необхідно звернути увагу, що обмінна ІА, якою обмінюються різні сторони, у будь-який момент є різною.

Автономна автентифікація

Автономна автентифікація характеризується обов'язковим використанням сертифікованих списків відкликаних сертифікатів, списків на відкликання сертифікатів, строкових сертифікатів і застосуванням інших методів відкликання перевірочної ІА (рис. 6.6). При автономній автентифікації одна чи декілька третіх довірчих сторін забезпечують автентифікацію без втручання в кожний етап автентифікації. У цьому режимі третя довірча сторона завчасно генерує та розподіляє сертифікати автономної автентифікації. У подальшому вони використовуються перевірником для підтвердження обміну автентифікації. Тому можна стверджувати, що обмін автентифікації в автономному режимі здійснюється анонімно без втручання уповноваженого, тобто третьої довірчої сторони.

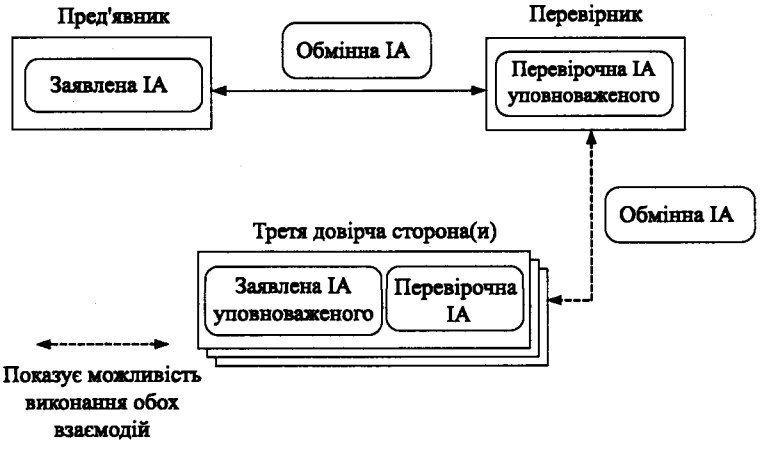

Рис. 6.6. Автономна автентифікація

Також відсутність необхідності безпосередньої взаємодії третіх довірчих сторін протягом автентифікації з пред'явником або перевірником дає можливість суттєво зменшити кількість необхідних взаємодій. Але для відкликання сертифікатів необхідно реалізувати додатково функції відстеження ланцюга сертифікатів, відновлення сертифікатів і перевірку сертифікованих списків відкликаних сертифікатів.

Пред'явник, що довіряє перевірнику

Якщо ідентифікаційні дані перевірника не автентифіковані, його надійність невідома. Можливе застосування політик безпеки, коли перевірнику можна довіряти. Але в більшості випадків перевірника необхідно розглядати як сторону, якій довіряти не можна.

6.3. КЛАСИФІКАЦІЯ КОМІТЕНТІВ І МЕХАНІЗМИ АВТЕНТИФІКАЦІЇ

Розглянемо основні ознаки, за якими може виконуватись автентифікація, та найбільш узагальнені структурні схеми взаємодії під час автентифікації.

Згідно з [210, 213], автентифікація, залежно від особливості її здійснення, може бути виконана такими двома способами:

1) комітента представляє пред'явник, що має особисті комунікаційні взаємовідносини з перевірником, тобто здійснюється об'єктна автентифікація;

2) комітент є ресурсом елементу даних, який доступний перевірнику, тобто здійснюється оригінальна ідентифікація даних.

За таких умов комітентів можна класифікувати за такими ознаками:

– згідно пасивних характеристик, які застосовуються, наприклад, такі біометричні ознаки, як відбиток пальця, сітчатка очей, особливості лиця тощо;

– у відповідності з інформацією, якою обмінюються пред'явник і перевірник, і здатністю її обробки;

– відповідно до здатності приймати та зберігати інформацію згідно з вимогами механізму, що застосовується;

– згідно з унікальністю можливостей у діях і поточним станом в інформаційному сенсі тощо.

Комітенти можуть застосовувати також і декілька (комбінацію) ознак, але для кожної ознаки повинен застосовуватись індивідуальний метод автентифікації, наприклад:

а) через контроль пасивних характеристик пред'явника;

б) комплексний контроль на основі застосування системи автентифікації з певною пропускною системою;

в) метод одночасного застосування конфіденційних даних, наприклад, особистого ключа ЕЦП та паролю доступу до нього;

г) визначення інформаційного стану, можливостей і наявності певних конфіденційних і критичних даних тощо.

Аналіз основних джерел показав, що при автентифікації можливі різні варіанти організації взаємодії окремих компонентів, автентифікація об'єктів і суб'єктів, наприклад, у локальній обчислювальній мережі (ЛОМ). Основними варіантами взаємодії можуть бути такі:

– між внутрішніми об'єктами (суб'єктами) ЛОМ взагалі, у перелік яких входять як об'єкти електронний засіб користувача, робоча станція (РС), такі об'єкти платформ, як сервери застосувань, сервери баз даних, сервер безпеки тощо;

– між внутрішніми об'єктами ЛОМ, перш за все серверами застосувань, сервери баз даних, сервер безпеки тощо, захист від НСД у яких здійснюється системою захисту інформації платформи;

– між внутрішніми і зовнішніми об'єктами різних ЛОМ тощо.

Розглянемо сутність та особливості криптографічних механізмів автентифікації для вказаних різних випадків. Причому під *криптографічним механізмом автентифікації* будемо розуміти конкретний процес, криптографічний протокол або криптографічний алгоритм, що використовується для реалізації визначених послуг автентифікації.

На рис. 6.7 і 6.8 наведено структурні схеми застосування комплексу у складі кожної з ЛОМ на об'єктах та організації взаємодії його окремих компонентів. Приклад структурної схеми взаємодії окремих компонентів між різними ЛОМ наведено на рис. 6.9.

На РС користувачів ЛОМ встановлюється програмний або програмно-апаратний комплекс захисту робочого місця (РС користувача) та підключений певний електронний засіб, наприклад, електронний ключ. На серверах застосунків (серверах застосувань) та серверах баз даних встановлюється певний програмний або програмно-апаратний комплекс захисту сервера застосунків (додатків) та підключений такий специфічний елемент, як модуль автентифікації ЛОМ. Сервер застосунків є одним із серверів, що забезпечує функціонування засобів захисту інформації в межах платформи.

На РС адміністратора безпеки ЛОМ також повинні бути встановлені такі самі компоненти автентифікації, що й на РС користувачів, а також частина програмного комплексу адміністрування безпеки.

На сервері безпеки ЛОМ повинні бути встановлені такі самі компоненти комплексу, що й на серверах функціональних і технологічних елементів, а також частпрограмного комплексу адміністрування безпеки.

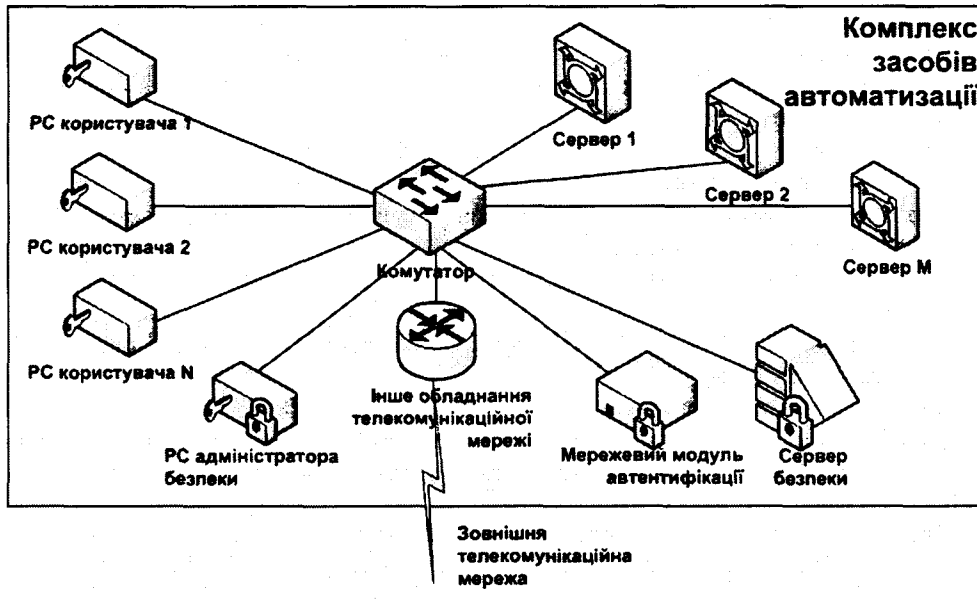

Рис. 6.7. Структурна схема застосування комплексу автентифікації

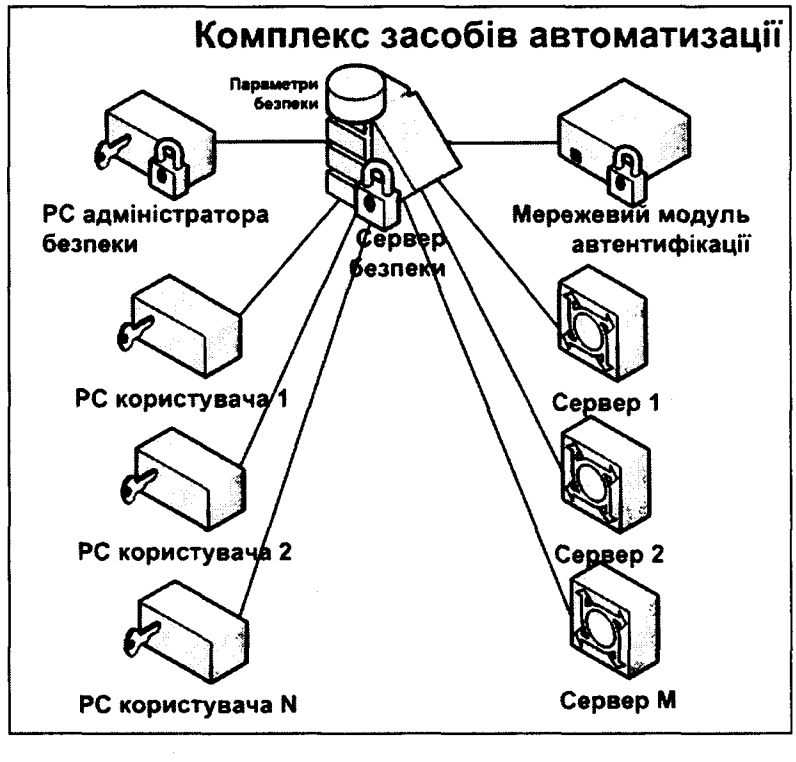

Рис. 6.8. Структурна схема організації взаємодії компонентів при автентифікації в середині ЛОМ

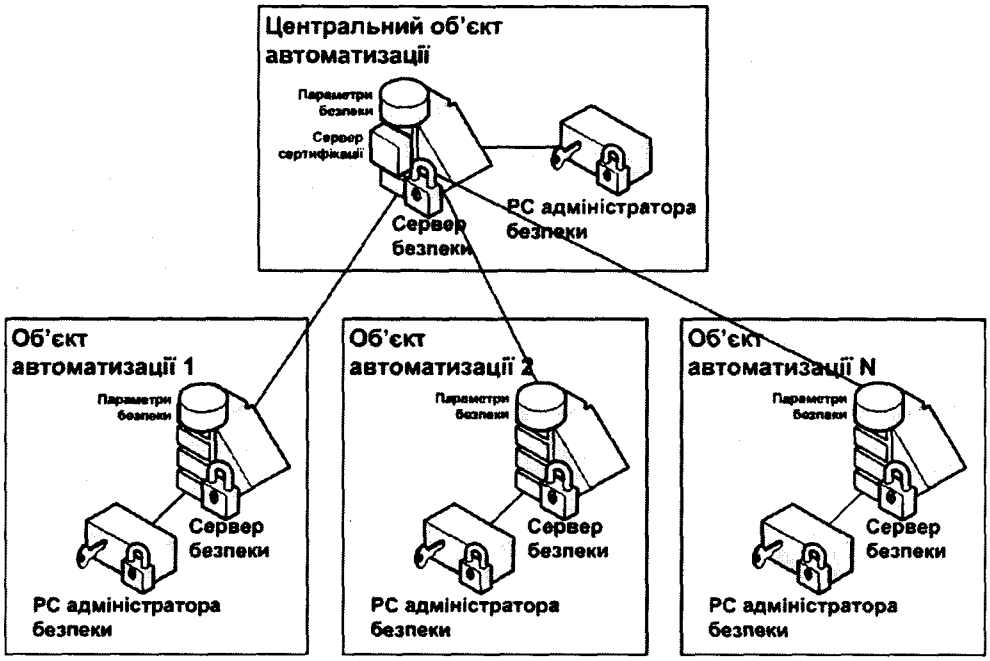

Рис. 6.9. Структурна схема організації взаємодії компонентів при автентифікації між різними ЛОМ

На сервері безпеки ЛОМ повинні бути встановлені такі самі компоненти комплексу, що й на серверах функціональних і технологічних елементів, а також частина програмного комплексу адміністрування безпеки.

Аналіз рис. 6.7 і 6.8 ЛОМ, у яких при організації взаємодії його окремих компонентів повинна здійснюватись автентифікація між внутрішніми об'єктами (суб'єктами) ЛОМ, дозволив виділити необхідні зв'язки. Так, згідно структурної схеми рис. 6.7 взаємодії окремих компонентів ЛОМ між різними об'єктами в процесі взаємодії взаємна автентифікація може здійснюватися між такими об'єктами:

- Сервер безпеки ЛОМ – РС ЛОМ вищого рівня;
- Сервер безпеки ЛОМ вищого рівня – РС сервера вищого рівня;
- Сервер безпеки ЛОМ вищого рівня – сервер ЛОМ нижчого рівня;
- Сервер безпеки ЛОМ вищого рівня – РС сервера ЛОМ;
- РС сервера безпеки ЛОМ – сервер безпеки своєї ЛОМ;
- РС сервера безпеки ЛОМ – сервер безпеки ЛОМ вищого рівня;
- РС сервера безпеки ЛОМ – РС сервера безпеки ЛОМ вищого рівня;
- Сервер безпеки ЛОМ – РС сервера безпеки тієї ж ЛОМ;
- Сервер безпеки ЛОМ – сервер безпеки ЛОМ вищого рівня тощо.

Зрозуміло, що не всі взаємодії з метою автентифікації є обов'язковими або дозволеними; окрім того, залежно від вимог при автентифікації можуть бути застосовані різні механізми та протоколи.

Таким чином, при подальшому розгляді систем автентифікації на основі ЕЦП необхідно провести:

– детальний аналіз і вибір криптографічного протоколу автентифікації РС і користувачів з електронним ключем і встановлення ключів згідно ДСТУ ISO/IEC 9798-3, ДСТУ ISO/IEC 15946-3 та ДСТУ ISO/IEC 11770-3;

– аналіз і вибір криптографічних протоколів автентифікації та встановлення ключів між РС і сервером застосувань та мережевим модулем автентифікації й сервером безпеки згідно ДСТУ ISO/IEC 9798-3, ДСТУ ISO/IEC 15946-3 та ДСТУ ISO/IEC 11770-3;

– аналіз і вибір криптографічних протоколів автентифікації та встановлення ключів між серверами безпеки (мережевими модулями автентифікації) різних ЛОМ згідно ДСТУ ISO/IEC 9798-3, ДСТУ ISO/IEC 15946-3 та ДСТУ ISO/IEC 11770-3.

6.4. ВИДИ АТАК НА АВТЕНТИФІКАЦІЮ

Усі відомі атаки відносно механізмів автентифікації можна розділити на два основних види [22, 36, 210]:

1) *атака типу «Повтор»* (*раніше передане повідомлення*) – при реалізації якої порушник спочатку записує обмінну ІА, її запам'ятовує, а потім пізніше її передають, тобто відтворюють;

2) *атака типу «Підміна»* – при реалізації якої обмінна ІА перехоплюється, підміняється та оперативно знову відтворюється, наприклад, передається перевірнику.

Структуру типів атак подано на рис. 6.10.

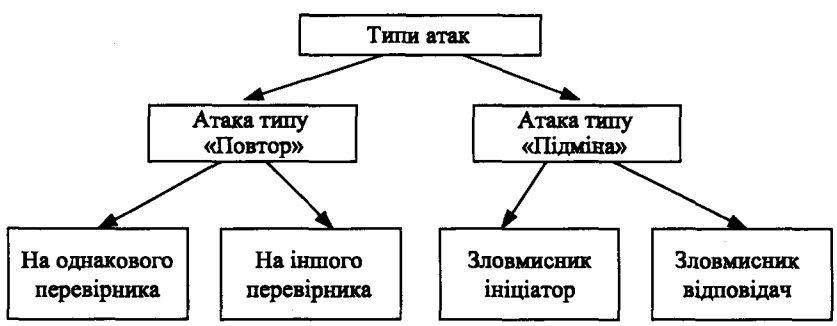

Рис. 6.10. Класифікація атак

6.4.1. Атаки типу «Повтор»

Атака типу «Повтор» на іншого перевірника можлива за умов знання декількома перевірниками перевірочної ІА комітента, наприклад, засобом її перехоплення, запам'ятовування та наступного відтворення. Таку атаку називають «раніше переданим повідомленням», оскільки, по суті, при її реалізації відтворюється санкціонована пред'явником ІА. У випадку успішної реалізації атаки типу «Повтор» її інколи називають «Маскарад».

Основним механізмом захисту проти атаки типу «Повтор» є використання запитів, наприклад паролів, маркерів з підписаною ІА тощо. При цьому запити генеруються перевірником, але перевірник не може використовувати однаковий запит на пароль більш ніж один раз, тому їх джерело повинне ґрунтуватися на випадкових послідовностях.

Для протистояння атаці типу «Повтор» можна використовувати унікальні числа, наприклад, номери передач, випадкові числа, а також робити запити паролів. При цьому унікальні числа генерує пред'явник, а при повторенні унікального числа або даних перевірник від нього відмовляється, тобто воно одним і тим самим перевірником не приймається.

Для протистояння атаці типу «Повтор» для різних перевірників, як правило, необхідно використовувати запити паролів. Для протистояння атаці типу «Повтор» для різних перевірників використовується обчислення заявленої ІА, наприклад, будь-яких характеристик, які є унікальними для перевірника, у першу чергу таких, як ім'я, IP-адреса або взагалі будь-які атрибути, що містять перевірочну ІА.

6.4.2. Атаки типу «Підміна», коли ініціатором є порушник

В атаці типу «Підміна» порушник повинен бути або є ініціатором автентифікації. Цей вид атак можливий тільки в тому випадку, коли ініціаторами можуть бути як пред'явник, так і перевірник. У процесі реалізації атаки пред'явник і перевірник обмінюються інформацією автентифікації через порушника. При цьому порушник для перевірника є пред'явником, а для пред'явника перевірником.

Метою атаки типу «Підміна» для порушника C є спроба представити себе для перевірника B як пред'явника A (рис. 6.11). Дії порушника при виконанні атаки можна представити таким чином.

1. Порушник починає одночасно взаємодіяти як з A, так і з B, причому:

а) порушник C представляється для A перевірником B і робить запит на його автентифікацію;

б) порушник C представляється для B пред'явником A і робить запит, щоб перевірник B його автентифікував.

2. При автентифікації пред'явник A насправді взаємодіє з порушником C, який видає себе за перевірника B, і таким чином порушник C одержує деяку інформацію від пред'явника A, яку потім використовує в процесі автентифікації з перевірником B.

3. Далі прі автентифікації перевірник B взаємодіє з порушником C, який видає себе за пред'явника A, і таким чином порушник C одержує деяку інформацію від перевірника B, яку потім використовує в процесі автентифікації з пред'явником A.

4. Надалі порушник C бере участь в процесі автентифікації з перевірником B як уже автентифікований пред'явник A.

Для протистояння атаці типу «Підміна», коли ініціатором є порушник, необхідно:

1) встановити з необхідною ймовірністю ініціатора взаємодії: це завжди або пред'явник, або перевірник;

2) щоб обмінна ІА, яка надається пред'явником, розрізнялася залежно від статусу пред'явника щодо ініціювання процесу автентифікації. Це дає можливість перевірнику відстежувати факт перехоплення обмінної ІА.

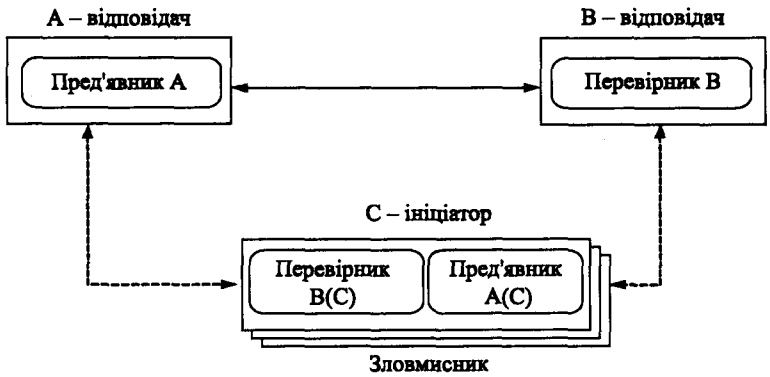

Рис. 6.11. Атака типу «Підміна», коли порушник є ініціатором

6.4.3. Атака типу «Підміна», у якій порушник є відповідачем

Для реалізації цієї атаки порушник повинен знаходитися посередині. Далі він перехоплює інформацію автентифікації та відправляє її, виконуючи ніби роль ініціатора. Атака типу «Підміна» може виконуватися (рис. 6.12):

1) у випадку, коли порушник чекає моменту, щоб його помилково прийняли за відповідача;

2) систематично, тобто коли порушник представляє себе як відповідача.

Для захисту від атаки типу «Підміна», у якій порушкник є відповідачем, можливо:

1) використовувати додаткові послуги, перш за все такі, як контроль цілісності або забезпечення таємності при додатковому обміні даними. При цьому обмінну ІА можна комбінувати з деякою іншою інформацією, що містить повноваження пред'явника та перевірника, наприклад, забезпечує легітимність частин для вироблення ключа. Вироблений ключ може потім використовуватися як ключ для механізмів забезпечення цілісності та конфіденційності, що засновані на криптографічних перетвореннях, наприклад, особистого ключа ЕЦП;

2) інтеграція адреси мережі в обмінну ІА (наприклад, у підпис мережевої адреси) у системах з контролюванням доставки пакетів даних за правильними адресами мереж.

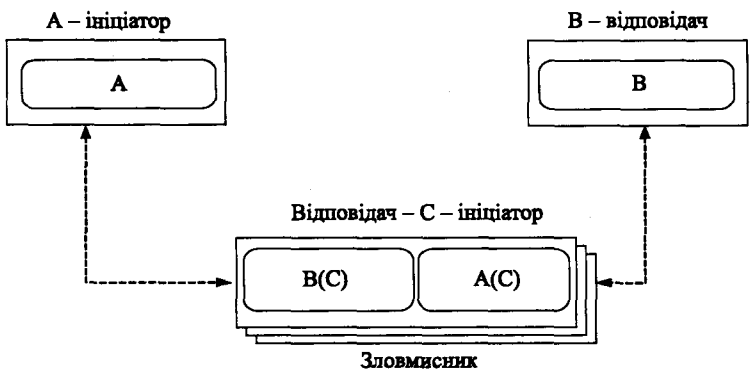

Рис. 6.12. Атака типу «Підміна», коли порушник є відповідачем

Моделі загроз, що розробляються з урахуванням моделі порушника, мають бути основою для формування політики безпеки, вибору та застосування механізмів і засобів захисту, а також організаційного забезпечення для функціонування комплексної системи захисту інформації.

6.5. ОСНОВНІ МЕХАНІЗМИ АВТЕНТИФІКАЦІЇ

6.5.1. Класифікація вразливостей

Відносно механізмів автентифікації можуть здійснюватись атаки, які обмежують їх ефективність. Механізми автентифікації, які можна використовувати для захисту у фазі передавання, можна класифікувати відносно загроз(и), проти яких ці механізми є невразливими. Як правило, механізми базуються на принципі автентифікації, який можна назвати «дещо відомо». Усі такі механізми можна застосовувати до об'єктів автентифікації, а механізми з цифровим підписом або геш-значенням можна застосовувати й для автентифікації джерела даних.

У [210] рекомендується використовувати такі класи механізмів автентифікації:

Клас 0 – Незахищений;

Клас 1 – Захищений від розкриття заявленої ІА;

Клас 2 – Захищений від розкриття заявленої ІА й атаки типу «Повтор» для різних перевірників;

Клас 3 – Захищений від розкриття заявленої ІА й атаки типу «Повтор» на одного перевірника;

Клас 4 – Захищений від розкриття заявленої ІА й атаки типу «Повтор» на одного перевірника або різних перевірників.

Під час розгляду механізмів автентифікації та аналізу криптографічних протоколів указане робиться з точки зору пред'явника, і тому пред'явник завжди є ініціатором. На основі цього застосовують усі класи механізмів направленої автентифікації, а потім проводиться уточнення, де ініціатором є перевірник, оскільки вони застосовуються для однонаправленої та взаємної автентифікації.

Для забезпечення захисту у випадку автентифікації джерела даних необхідно використовувати цифровий відбиток, наприклад ЕЦП, що досягається за рахунок використання алгоритму асиметричного шифрування. Може також застосовуватись симетричне шифрування, наприклад, у вигляді коду автентифікації повідомлення (імітовставки), або криптографічного контрольного значення від даних, що виготовлені з використанням особистого ключа ЕЦП.

6.5.2 Класи механізмів автентифікації, коли пред'явник є ініціатором

6.5.2.1. Незахищений клас автентифікації 0

У механізмах автентифікації класу 0 заявлена ІА відправляється як обмінна ІА від пред'явника перевірнику разом із розпізнавальним ідентифікатором. У класі 0 для автентифікації застосовуються симетричні криптоперетворення. Механізми автентифікації цього класу вразливі до розкриття інформації автентифікації та атаки типу «Повтор».

На рис. 6.13 наведено механізм формування та передачі–приймання маркера – обмінної ІА безпосередньо з вхідних даних.

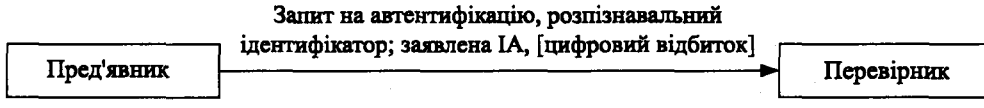

Рис. *6.13.* Механізм класу 0 (незахищений)

6.5.2.2. Клас автентифікації 1 – Захищений від розкриття заявленої ІА

При застосуванні клас автентифікації 1 механізмів автентифікації забезпечує захист від розкриття заявленої ІА і може застосовуватися для автентифікації джерела даних та об'єкта.

Ці механізми автентифікації ґрунтуються на використанні функції перетворення, причому заявлена ІА може комбінуватися з розпізнавальним ідентифікатором. Потім отримані дані перетворюються з використанням цієї функції перетворення, а одержане значення передається разом із розпізнавальним ідентифікатором. Відкрите значення заявленої інформації не передається по комунікаційному каналу.

Основними механізмами автентифікації класу є такі:

1) передача паролю, перетвореного за допомогою однонаправленої функції, наприклад, у вигляді криптографічного контрольного значення або геш-значення.

2) передача електронного підпису, захищеного конфіденційним ключем;

3) передача паролю, який зашифровано на конфіденційному ключі;

4) передача цифрового підпису, який вироблено з використанням особистого ключа.

Механізми автентифікації класу 1 уразливі проти атаки типу «Повтор». Наприклад, пароль, що передається, можна знов відтворювати на рівні протоколу обміну, але відкритий пароль, який використовується на рівні системного інтерфейсу, не розкривається.

У цьому випадку як вхідні дані криптографічного перетворення для генерування обмінної ІА (маркер) використовується заявлена ІА та, за необхідності, розпізнавальний ідентифікатор та/або електронний підпис (цифровий відбиток) (рис. 6.14).

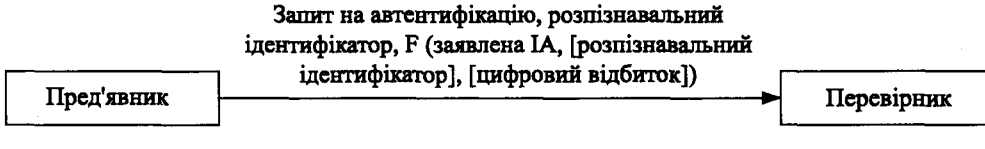

Рис. 6.14. Механізм класу 1 – захищений від розкриття заявленої ІА(ЗРІА)

Для криптографічного перетворення $F()$ при генеруванні обмінної ІА може застосовуватись:

1) у разі використання однонаправленої функції ЗРІА перевірка ґрунтується на використанні замість заявленої ІА перевірочної ІА та наступного порівняння з одержаною обмінною ІА;

2) у разі використання симетричного шифрування ЗРІА перевірка ґрунтується на використанні для розшифрування одержаної обмінної ІА перевірочної ІА, а потім перевірці справжності розшифрованих даних шляхом перевірки збігу розшифрованого розпізнавального ідентифікатора та розпізнавального ідентифікатора пред'явника, правильність цифрового відбитку (електронного підпису), паролю та постійних значень;

3) у разі використання цифрового підпису ЗРІА перевірка ґрунтується на обчисленні цифрового відбитку від одержаних даних та використанні перевірочної ІА для перевірки того, що одержаний підпис є дійсним підписом для даного відбитку (електронного підпису).

Додатково, у випадку автентифікації джерела даних, цифровий відбиток (електронний підпис), який одержано з обмінної ІА, порівнюють з генерованим перевірником цифровим відбитком даних. Коли розпізнавальний ідентифікатор комбінують із заявленою ІА, складність екзистенційної (exhaustive) атаки суттєво підвищується. Причому атаку, за необхідністю, можна вести одноразово тільки на визначеного комітента, замість виконання атаки на всіх комітентів разом.

Для надання конфіденційності ІА функція перетворення повинна бути однонаправленою, або мати експоненційну складність зворотного перетворення для частин, які не повинні мати доступ до конфіденційної заявленої ІА (цифрового відбитку).

6.5.2.3. Клас автентифікації 2 – Захищений від розкриття заявленої ІА та атаки типу «Повтор» на різних перевірників

Клас 2 механізмів автентифікації забезпечує при його застосуванні захист від розкриття заявленої ІА та атак типу «Повтор» на різних перевірників, але не може забезпечити захист від атак типу «Повтор» з одним перевірником. Цей клас механізмів ідентичний Класу 1, але додатково на вхід функції перетворення, для надання додаткового захисту, подається унікальна характеристика обраного перевірника.

6.5.2.4. Клас автентифікації 3 – Захищений від розкриття заявленої ІА та атаки типу «Повтор» на одного перевірника

Цей клас 3 механізмів автентифікації забезпечує захист від розкриття заявленої ІА та атак типу «Повтор» на одного перевірника.

Механізми цього класу ґрунтуються на використанні для надання додаткового захисту від атаки типу «Повтор» на одного перевірника функції перетворення разом з унікальною інформацією. Заявлена ІА та унікальний номер захищаються з використанням криптографічних перетворень і передаються разом з розпізнавальним ідентифікатором.

Для унікального представлення можна застосовувати:

1) *випадкове або псевдовипадкове число* – число, яке не може бути повторено навмисне впродовж життєвого циклу заявленої ІА (з імовірністю більше заданої). Випадкове або псевдовипадкове число певної довжини дозволяє зменшити ймовірність того, що таке число вже використовувалося;

2) *позначка (мітка) часу* є унікальним числом упродовж життєвого циклу заявленої ІА, що одержано з довірчого джерела. Старі мітки часу, або мітки часу, які попередньо використовували, виявляються з великою ймовірністю.

3) *лічильник* – значенням лічильника є унікальне число, яке постійно збільшується, доки використовують однакову заявлену ІА.

4) *криптографічне зв'язування* – унікальне число є зв'язаним значенням, якщо воно одержане зі змісту попередніх даних, що передаються між пред'явником і перевірником, шляхом застосування в деякий момент часу.

Унікальність числа, що отримане зв'язуванням, може гарантуватися пред'явником за рахунок конкатенації його з даними, що є унікальними для пред'явника (наприклад такого, як особистий розпізнавальний ідентифікатор пред'явника). За необхідності для створення унікального числа можна використовувати комбінацію цих методів.

Як функції перетворення в 3-му класі можуть застосовуватись:

1) *однонаправлена функція.* У цьому випадку унікальне число, заявлена ІА та, можливо, розпізнавальний ідентифікатор перетворюються за допомогою однонаправленої функції. Унікальне число також передається перевірнику, тому він може виконати таке саме перетворення;

2) *асиметричний алгоритм.* За цих умов заявлена ІА є особистим ключем, при цьому унікальне число підписується на особистому ключі;

3) *симетричний ключ,* коли заявлена ІА є таємним ключем, при цьому унікальне число зашифровується на таємному ключі.

Розглянутий клас механізмів застосовується для автентифікації джерела даних та об'єкта. Унікальне число генерується за допомогою ЗРІА генерування, наприклад, для цього може використовуватись (рис. 6.15):

1) унікальне число;

2) заявлена ІА;

3) розпізнавальний ідентифікатор (необов'язково);

4) цифровий відбиток (у випадку автентифікації джерела даних).

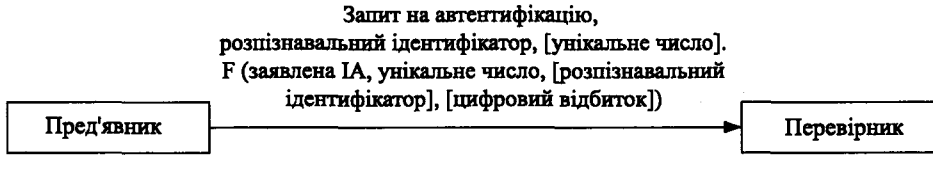

Рис. 6.15. Клас 3 – Механізм з унікальним числом

Необхідно відзначити, що в процесі перевірки виконується розшифрування та перевірка дійсності обмінної ІА з використанням перевірочної ІА, що описана в Класі 1. Також перевіряється унікальність одержаного унікального числа. Якщо число було одержане раніше, тоді видається повідомлення про повтор унікального числа. При використанні автентифікації джерела даних додатково порівнюється цифровий відбиток (електронний підпис) в обмінній ІА та генерований з одержаних даних перевірником.

6.5.2.5. Клас автентифікації 4 – Захищений від розкриття заявленої ІА та атаки типу «Повтор» на одного перевірника та різних перевірників

У класі автентифікації 4 введено 4 підкласи механізмів автентифікації – 4*a*, 4*b*, 4*c* та 4*d*. Розглянемо вимоги та умови реалізації цих класів з метою реалізації механізмів автентифікації.

Проміжний клас 4a – Механізми автентифікації з унікальним числом

Цей проміжний клас ідентичний класу 3, але додатково на вхід функції перетворення для надання додаткового захисту подається унікальна характеристика обраного перевірника.

Проміжний клас 4b – Механізми автентифікації із запитом паролю

Цей проміжний клас 4*b* гарантує захист від атак типу «Повтор», тобто будь-яка спроба здійснити автентифікацію шляхом повтору обмінної ІА з наперед визначеною (великою) ймовірністю закінчиться невдачею. Механізм захисту діє таким чином. У відповідь на запит пред'явника про автентифікацію перевірник у свою чергу генерує та передає пред'явнику у формі елемента даних з унікальним значенням запит на перевірку паролю. Пред'явник перетворює інформацію запиту на перевірку пароля та заявлену ІА за допомогою деякої функції, а потім повертає результуюче значення цієї функції перевірнику.

Механізми із запитом паролю ґрунтуються на трьох обмінах інформацією між пред'явником та перевірником:

1) відправка запиту на автентифікацію від пред'явника до перевірника;

2) генерування запиту на перевірку пароля та відправка його від перевірника до пред'явника;

3) відправка від пред'явника до перевірника відповіді, що отримана за допомогою деякої визначеної функції F від заявленої ІА, можливо, комбінованої з розпізнавальним ідентифікатором, та інформації запиту на перевірку паролю.

У загальному випадку розпізнавальний ідентифікатор може відсилатися або в запиті на автентифікацію, або з кінцевою відповіддю.

Як функція перетворення F для механізмів із запитом паролю можуть бути використані:

1) однонаправлена функція – коли запит на перевірку паролю та обмінна ІА перетворюються за допомогою однонаправленої функції;

2) асиметричний алгоритм – коли заявлена ІА є особистим ключем, при цьому запит на перевірку пароля підписується на особистому ключі;

3) симетричний алгоритм – коли заявлена ІА є таємним ключем, при цьому запит на перевірку паролю зашифровують на таємному ключі.

Ці механізми відомі як спеціалізовані механізми із запитом паролю. У цьому випадку розпізнавальний ідентифікатор обов'язково присутній у запиті на автентифікацію, при цьому з'являється четверта можлива функція перетворення – некриптографічний алгоритм. Одним із таких прикладів є використання таблиці пар одержаних запитів на перевірку пароля. Іншими прикладами є біометричні схеми, такі як система повтору голосу тощо.

Цей проміжний клас 4*b* використовується для автентифікації джерела даних та об'єктів.

Також необхідно відзначити, що у вказаних механізмах запит на автентифікацію повинен супроводжуватися розпізнавальним ідентифікатором.

При використанні однонаправленої функції для перевірки одержаних даних на третьому проході (рис. 6.16) при перевірці замість заявленої ІА використовується перевірочна ІА. При цьому перевірник повинен мати розпізнавальний ідентифікатор і дату, для якої застосовується послуга.

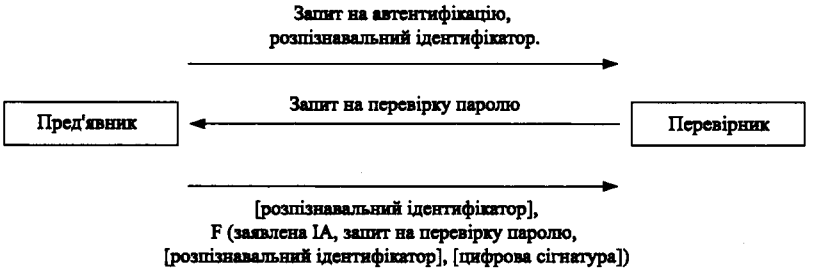

Рис. 6.16. Проміжний клас 4*b* – Механізми із запитом на перевірку паролю

Проміжний клас 4c – Спеціалізовані механізми автентифікації із запитом паролю та шифруванням

Спеціалізовані механізми із запитом паролю та шифруванням ґрунтуються на трьох обмінах інформацією між пред'явником і перевірником. Суть механізмів у такому:

1) відправка запиту на автентифікацію та розпізнавального ідентифікатора від пред'явника до перевірника;

2) генерування запиту на перевірку пароля та перевірочну ІА, можливо, разом із розпізнавальним ідентифікатором, та відправка його від перевірника до пред'явника;

3) відправка від пред'явника до перевірника відповіді, що отримана за допомогою деякої визначеної функції F від заявленої ІА, можливо, комбінованої з розпізнавальним ідентифікатором, та інформації запиту на перевірку паролю.

Як функція перетворення F для механізмів із запитом паролю та шифруванням можуть бути використані:

1) асиметричний алгоритм, коли заявлена ІА є особистим ключем, при цьому запит на перевірку пароля зашифровується на особистому ключі;

2) симетричний алгоритм, коли заявлена ІА є таємним ключем, при цьому запит на перевірку паролю зашифровують на таємному ключі.

Цей проміжний клас використовується для автентифікації джерела даних та об'єктів.

Приклад реалізації спеціалізованих механізмів із запитом пароля та шифруванням наведено на рис. 6.17.

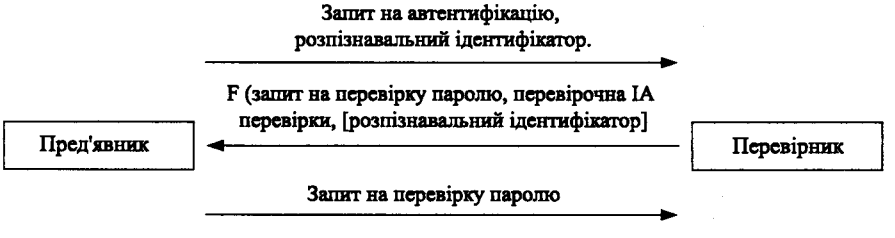

Рис. 6.17. Спеціалізовані механізми із запитом паролю та шифруванням

Проміжний клас 4d – Механізми з обчисленням відповіді

Механізми з обчисленням відповіді ґрунтуються на трьох обмінах інформацією між пред'явником і перевірником. Суть механізмів полягає в такому:

1) відправка запиту на автентифікацію від пред'явника до перевірника з вибором значень для відбору та інформації про ідентифікаційні дані;

2) генерування перевірником запиту на перевірку пароля та перевірочну ІА, яка містить інформацію про те, яке значення обрано перевірником, та відправка його пред'явнику;

3) відправка пред'явником перевірнику відповіді, що містить перетворене за допомогою деякої визначеної функції унікальне число, запит на перевірку паролю або обрані значення для обчислення відповіді та заявлену ІА.

Для надання більшого рівня гарантій ідентифікаційним даним обміни у вказаних механізмах можуть повторюватися. При застосуванні механізмів класу 4*d* забезпечується захист від атак типу «Маскарад», що можуть здійснюватись порушником. Порушник може обчислити коректну відповідь для деяких значень, але не для всіх, які може обрати перевірник. Також необхідно враховувати, що при здійсненні тільки одного обміну перевірник може обрати значення, для якого порушник знає коректну відповідь. При збільшенні числа обмінів між пред'явником та перевірником імовірність успішного виконання такої атаки зменшується.

Таким чином, на першому етапі пред'явник спочатку генерує унікальне число, вибирає значення та поміщає їх в обмінну ІА (рис. 6.18). Перевірник також обирає з відповідної множини та генерує запит значення на перевірку пароля для формування другої обмінної ІА.

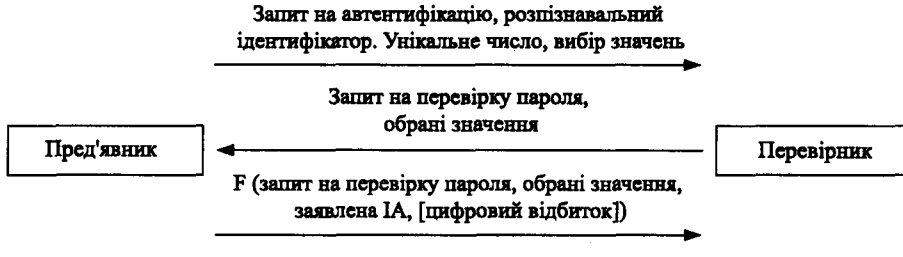

Рис. 6.18. Проміжний клас 4*d* – Механізми з обчисленням відповіді

Пред'явник виконує перетворення над запитом на перевірку пароля або обраними значеннями, використовуючи заявлену ІА, та надсилає результати перетворень перевірнику. Після отримання від пред'явника маркера перевірник виконує, використовуючи перевірочну ІА, зворотне перетворення та перевіряє одержані значення згідно з механізмом автентифікації.

6.5.3. Класи механізмів автентифікації, де перевірник є ініціатором

Механізми, що наведено нижче, можуть застосовуватися для випадків, коли ініціатором обмінів при автентифікації виступає перевірник. У табл. 6.1 наведено кількість передавань для випадків, коли ініціатором виступає пред'явник або перевірник.

Використання сертифікатів автентифікації

Механізми автентифікації, у яких ініціатором є перевірник, можна класифікувати за методами одержання перевірочної ІА. Для реалізації механізмів можуть використовуватись:

1) інтерактивні сертифікати автентифікації;

2) автономні сертифікати автентифікації;

3) перевірочна ІА, яка надається додатковим шляхом, наприклад, з використанням захищених каналів.

У механізмах, що розглядаються, сертифікат автентифікації надає доказ того, що ТДС здійснила зв'язок між даним розпізнавальним ідентифікатором та спеціалізованою перевірочною ІА.

6.5.4. Взаємна автентифікація

Взаємна автентифікація може здійснюватись із застосуванням однопрохідних механізмів (обмінів). Для цього можуть застосовуватись проміжні класи механізмів 1, 2, 3 та 4*a*. Причому обмін необхідно здійснювати в обох напрямках.

Так само і для проміжного класу механізмів автентифікації 4*b* однаковий тип механізму можна використовувати в обох напрямках, тобто перший запит на перевірку пароля може надсилатися разом із запитом на автентифікацію. Далі перетворення першого запиту на перевірку пароля повинне надсилатись разом з другим запитом на перевірку пароля (рис. 6.19). Проміжний клас механізму 4*b*, при його застосуванні в обох напрямках вимагає однакового числа обмінів, тобто як і для звичайної направленої автентифікації.

При використанні проміжного класу 4*c* перетворення першого запиту на перевірку пароля може надсилатися разом із запитом на автентифікацію, а перетворення другого запиту на перевірку пароля може надсилатися з першим запитом на перевірку пароля.

Проміжний клас механізмів 4*b* може також використовуватися разом із механізмами класу 4*c*. У цьому випадку два запити на перевірку пароля поміщають разом із даними на передачу. У випадку симетричного шифрування заявлена ІА та перевірочна ІА є однаковими, а перетворення виконується тільки один раз. У разі асиметричного шифрування виконуються два перетворення окремо для перевірочної ІА та заявленої ІА.

У проміжному класі 4*d* для реалізації направленої автентифікації необхідно не менше трьох обмінів між пред'явником та перевірником, у той час як для взаємної автентифікації потрібно щонайменше чотири передавання.

Необхідно враховувати, що передавання розпізнавальних ідентифікаторів у цих механізмах узгоджуються згідно з проміжними класами.

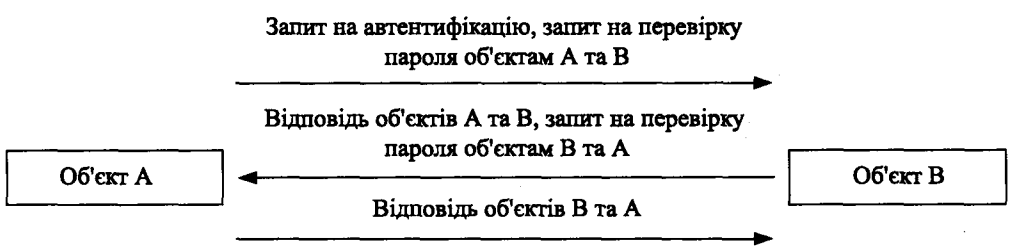

Рис. 6.19. Взаємна автентифікація з використанням механізмів із запитом на перевірку пароля (об'єкт А – ініціатор процесу автентифікації, об'єкт В – відповідач у процесі автентифікації)

6.5.5. Загальна характеристика класів

У табл. 6.1 подано характеристики та можливі вразливості відносно різних класів і проміжних класів.

Таблиця 6.1. **Характеристики класів захищеності**

Проміжний клас уразливості	0	1	2	3	4a	4b	4c	4d
Розкриття заявленої ІА	Так	Ні	Ні	Ні	Ні	Ні	Ні	Ні
Атака типу «Повтор» на різних перевірників	Так	Так	Ні	Так	Ні	Ні	Ні	Ні
Атака типу «Повтор» на одного перевірника	Так	Так	Так	Ні	Ні	Ні	Ні	Ні
Атака типу «Підміна» з порушником-ініціатором	Ні	Ні	Ні	Ні	Ні	Ні	Ні	Ні
Атака типу «Підміна», у якій порушник є відповідачем	Так	Ні	Ні	Ні	Ні	Ні	Ні	Ні
Характеристики:								
– симетричні/ асиметричні	Сим.	Будь-яке	Будь-яке	Будь-яке	Будь-яке	Будь-яке	Будь-яке	Асим.
– криптографічні (Так)/ некриптографічні (Ні)	Ні	Будь-яке	Будь-яке	Будь-яке	Будь-яке	Будь-яке	Так	Так
Кількість передавань:								
– пред'явник – ініціатор	1	1	1	1	1	3	3	3
– перевірник – ініціатор	2	2	2	2	2	2	4	4
Надання автентифікації джерела даних	Так	Так	Так	Так	Так	Так	Ні	Так

6.6. ВЗАЄМОДІЯ З ІНШИМИ ПОСЛУГАМИ/ МЕХАНІЗМАМИ

Реалізація механізмів автентифікації з наданням безпосередньої послуги автентифікації об'єктів і суб'єктів може бути безпосередньо або деякою мірою суміщена з іншими послугами – доступності, цілісності, конфіденційності та неспростовності. Розглянемо їх суть.

6.6.1. Контроль доступу

Перед наданням дозволу на доступ до інформації необхідно автентифікувати об'єкт чи суб'єкт. При цьому результати проходження автентифікації забезпечують доступ до послуги контролю доступу.

6.6.2. Цілісність даних

Протокол автентифікації може виконуватись разом із послугою надання цілісності даних. У цьому випадку може бути гарантовано нерозривність автентифікації та зроблено підтвердження джерела даних.

Також деякі механізми автентифікації можуть ґрунтуватись на розділенні ключової інформації (явно чи неявно), що у свою чергу можна використовувати для надання послуги цілісності. При неявному визначенні ключової інформації, шлях одержання її з переданих даних повинен бути відомим або визначатися під час обміну при автентифікації. При явному визначенні ключової інформації при автентифікації додатково необхідно передавати під час обміну дані в одному із двох напрямків.

6.6.3. Конфіденційність даних

Механізми автентифікації можуть також використовуватися для розподілення ключової інформації (явно чи неявно), що можна використовувати для надання послуги конфіденційності. При неявному визначенні ключової інформації шлях одержання цих ключових даних з переданих даних має бути відомим або визначатися під час обміну при автентифікації. При явному визначенні ключової інформації додатково під час обміну при автентифікації необхідно передавати дані в одному із двох напрямків.

6.6.4. Неспростовність

Деякі механізми автентифікації можуть використовуватися для розподілення ключового матеріалу (явно чи неявно), що можна використовувати для надання послуги неспростовності. При неявному визначенні такого ключового матеріалу шлях одержання цього ключового матеріалу з переданих даних має бути відомим або визначатися під час обміну при автентифікації. При явному визначенні такого ключового матеріалу під час обміну при автентифікації додатково необхідно передавати дані в одному із двох напрямків.

6.7. ЗАГАЛЬНА МОДЕЛЬ ЗАГРОЗ

Основними додатками теорії автентичності є забезпечення цілісності й справжності інформації та ресурсів, надання послуг неспростовності й автентичності (справжності) джерела інформації [7–10, 51, 210–213].

6.7.1. Спрощена модель загроз

Раніше основні концепції автентифікації з метою захисту від НСД розглядалися, по суті, в частині криптографічних протоколів. Наведені концептуальні положення можуть бути застосовані й до інформації, що обробляється. Уведемо та розглянемо спрощену модель загроз.

На рис. 6.20 наведена спрощена схема моделі взаємної недовіри та взаємного захисту [7, 10].

На рис. 6.20 позначено:

D_1, D_2 – джерела інформації;

ЗЗІ – засіб захисту інформації;

ТС (НІ) – телекомунікаційна система (носій інформації);

КРА – криптоаналітик (порушник);

ДК – джерело ключів.

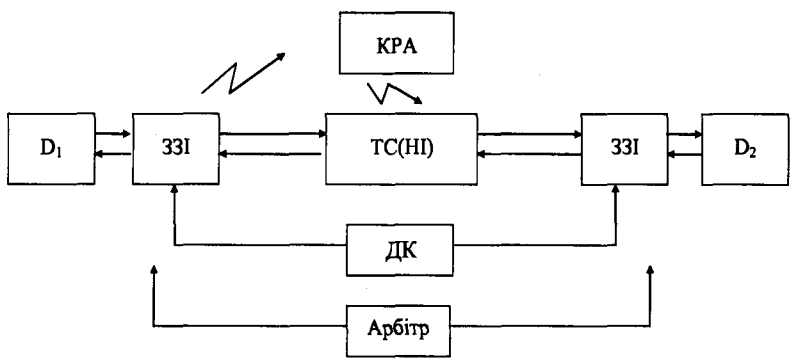

Рис. 6.20. Спрощена схема моделі взаємної недовіри та взаємного захисту

Виділимо 4 суб'єкти:

1) джерело D_1;

2) порушник (криптоаналітик – КРА);

3) арбітр;

4) джерело D_2.

Вони не довіряють один одному. Так, D_1 може зробити спробу обманути D_2.

Основні загрози, що може реалізувати джерело D_1:

1) D_1 формує повідомлення M_i, а потім відмовляється від факту передачі його в мережу;

2) джерело D_1 стверджує, що він сформував деяку інформацію M_i і передав у мережу, а насправді він її не формував і не передавав;

3) D_1 стверджує, що він сформував і передав інформацію M_i у визначений час, хоча насправді він сформував і передав її в інший час;

4) D_1 формує та передає інформацію M_i', а потім стверджує, що була передана інформація M_i, тощо;

Джерело D_2 також може робити спроби обманути D_1.

Основні загрози, що може реалізувати джерело D_2:

1) D_2 сам формує деяку M_i' інформацію, а потім D_2 стверджує, що він її отримав від D_1;

2) D_2 отримує M_i інформацію від D_1, модифікує її в M_i', а потім стверджує, що він отримав цю інформацію від D_1;

3) D_2 стверджує, що він отримав інформацію M_i в момент часу t_j, а насправді він отримав інформацію в час t_i;

4) D_2 отримує інформацію M_i, а потім стверджує, що він її не отримав, тощо.

Основні загрози, що може реалізувати КРА:

1) імітація помилкового повідомлення M_i: КРА у момент часу, коли D_1 пасивний, створює помилкову M_i інформацію і передає її D_2;

2) модифікація правильної інформації M_i: у випадку, якщо D_1 передає D_2 деяку інформацію M_i, КРА модифікує інформацію M_i в M_i' і передає її D_2;

3) нав'язування раніше створеної інформації (повтор), тобто КРА в будь-який момент часу t_j передає її ще раз D_2, коли D_1 пасивний;

4) передача хибних команд керування мережними службами, помилкові команди керування ключами, підміна сертифікатів тощо.

Арбітра також можна вважати порушником і не довіряти йому, від нього потрібно також захищатися.

Задача систем забезпечення цілісності та спостережливості інформації – мінімізувати втрати при дії безлічі загроз.

6.7.2. Вступ у теорію автентичності Сімонсона

У 70-ті роки вперше була опублікована теорія захисту від обману (автентичності), що отримала назву теорії Сімонсона [214].

Суть теорії Сімонсона. У теорії Сімонсона вважається, що два користувачі D_1 і D_2 взаємодіють між собою по відкритій телекомунікаційній системі (ТС) і для обміну між ними виділяється одноразовий ключ автентифікації.

Вважатимемо, що простір повідомлень M_i може бути сформований з n_{M_i} повідомлень.

Захист інформації здійснюється в ЗЗІ (рис. 6.1).

У ЗЗІ формується криптограма:

$$C_i = F^+(M_i, K_j^+, \Pr). \tag{6.1}$$

У подальшому C_i передається по ТС, а потім ЗЗІ відновлює інформацію:

$$M_i' = F^-(C_i', K_j^-, \Pr). \tag{6.2}$$

Вважатимемо, що джерело криптограм формує n_{C_i} криптограм. Якщо КРА сформував безліч криптограм n_{C_i} і одну з них передав, то він може обманути з імовірністю [7, 214]:

$$P_{обм} = \frac{n_M}{n_C}, \tag{6.3}$$

де $P_{обм}$ – імовірність обману.

Якщо $n_M = n_C$, то ймовірність нав'язування повідомлення, тобто обману, дорівнює 1.

Наша задача – зменшити $P_{обм}$, для цього необхідно збільшити простір криптограм:

$$n_M < n_C, \text{ або } n_M << n_C. \tag{6.4}$$

Для створення безумовно стійкої системи $n_C \to \infty$, тоді час передачі інформації буде $t \to \infty$. Із зазначеного випливає, що ніколи не можна реалізувати криптографічний захист, коли $P_{обм} = 0$, можна тільки зменшити $P_{обм}$.

У теорії Сімонсона прийнято визначати ймовірність обману, використовуючи (6.3).

Якщо $n_M < n_C$, то в системі може бути нав'язане повідомлення випадкового змісту. Так, КРА в моделі рис. 6.1 може реалізувати такі загрози:

– імітація, P_i – імовірність імітації;

– підміна, P_n – імовірність підміни;

– передача раніше переданого повідомлення з імовірністю $P_{рп}$.

P_Σ – імовірність усіх останніх загроз.

При проектуванні та оцінці автентичності необхідно визначити, яка загроза є найбільш небезпечною.

У своїй теорії Сімонсон здійснює оцінку однієї з найбільш небезпечних загроз:

$$P_{обм} = \max (P_i, P_n, P_{рп}, P_\Sigma). \tag{6.5}$$

Він визначив $P_{обм}$ як максимальну загрозу з усієї множини загроз.

Вважатимемо, що джерело D_1 разом із ЗЗІ формують криптограму C_i та відомий апріорний ряд $P(C_i)$ для $i = \overline{1, n_c}$. Якщо відома $P(C_i)$, можна знайти ентропію джерела криптограм D_1:

$$H(C) = -\sum_{i=1}^{n} P(C_i) \log P(C_i). \tag{6.6}$$

КРА, перехоплюючи криптограми, намагається визначити ключ автентифікації, який використовується для забезпечення цілісності та справжності (достовірності). Незнання КРА відносно ключа або надмірності, внесеної в криптограму, можна записати як умовну ентропію, що ключ K_i використовується для криптограми C_i:

$$H(C/K) = -\sum_i \sum_j P(C_i, K_j) \log_2 P(C_i/K_j) = \tag{6.7}$$

$$= -\sum_{i=1} \sum_{j=1} P(K_j) P(C_i/K_j) \log_2 P(C_i/K_j),$$

причому $P(C_i/K_j)$ вважаємо відомою.

Визначимо, яку кількість інформації ΔI отримав КРА при переході від $H(C)$ до $H(C/K)$:

$$\Delta I(C, K) = H(C) - H(C/K).$$

Сімонсон показав, що для моделі (6.5), коли вибирається тільки одна загроза, ймовірність обману може бути обчислена за формулою:

$$\log_2 P_{обм} \geq -\Delta I(C,K). \tag{6.8}$$

Знайдемо із (6.8) $P_{обм}$:

$$P_{обм} \geq 2^{-\Delta I(C,K)}. \tag{6.9}$$

Вираз (6.9) у теорії Сімонсона визначає межу ймовірностей обману в системі. Розглянемо (6.9).

Криптосистеми, у яких досягається рівність (6.9), називаються *системами з найкращим способом автентичності* (*повністю автентичні*).

Для зменшення ймовірності обману необхідно збільшувати $\Delta I(C,K)$, тобто кількість інформації, що міститься в криптограмі про ключ автентифікації.

Для забезпечення цілісності та достовірності необхідно вводити додатковий ключ автентифікації K_a. Таким чином, у нашій системі з'являється 2 ключі – ключ шифрування $K_ш$ та ключ автентифікації K_a.

Імовірність обману становить:

$$P_{обм} \geq 2^{-l_i}, \tag{6.10}$$

де l_i – довжина імітоприкладки (коду автентифікації).

Розглянемо (6.3) та (6.10). Нехай довжина повідомлення буде l_M бітів. Довжина контрольної суми l_i. Тоді довжина криптограми:

$$l_c = l_м + l_i. \tag{6.11}$$

Для двійкового алфавіту

$$n_м = 2^{l_м};\ n_c = 2^{l_c} = 2^{l_м + l_i}. \tag{6.12}$$

Підставимо (6.12) у (6.3):

$$P_{обм} \geq \frac{2^{l_м}}{2^{l_м + l_c}} = 2^{-l_i}. \tag{6.13}$$

Тобто (6.13) співпадає з (6.10).

Приклад оцінки ймовірності обману

Оцінимо ймовірність обману, якщо для забезпечення цілісності та справжності використовується електронний цифровий підпис (ЕЦП) ДСТУ 4145-2002.

Розв'язування прикладу

Спочатку зробимо оцінку, використовуючи границю Сімонсона.

$P_{обм} > 2^{-l_{ЦП}}$, де $l_{ЦП} = 160$ – довжина ЕЦП, що використовується.

$P_{обм} > 2^{-160} \approx 6{,}8 \cdot 10^{-49}$.

Відомо також, що ймовірність обману можна визначити як

$$P_{обм} > \frac{2^{l_м}}{2^{l_м + l_{ЦП}}}, \tag{6.14}$$

де l_M – довжина підписуваної інформації, а $l_{ЦП}$ – довжина ЕЦП.

Із цього співвідношення маємо:

$$P_{обм} > 2^{l_м} \cdot 2^{-l_м - l_{ЦП}} = 2^{l_{ЦП}}. \tag{6.15}$$

Таким чином, оцінка Сімонсона співпадає з останньою, отриманою через розмір множин повідомлень і повідомлень, автентифікованих за допомогою ЕЦП.

6.8. МЕТОДИ АВТЕНТИФІКАЦІЇ З ВИКОРИСТАННЯМ ЕЛЕКТРОННИХ ЗАСОБІВ ТА ЕЦП

6.8.1. Методи автентифікації з використанням ЕЗ

Як зазначалося раніше, в процесі автентифікації здійснюється перевірка дійсності суб'єкта, що робить запит на доступ до інформації чи ресурсів системи за пред'явленим ним ідентифікатором [210, 215, 216]. За такої умови як ідентифікатор виступають ознака автентифікації суб'єкта та/або електронний засіб, наприклад електронний ключ, старт-карта тощо. Згідно з 6.6 якісним механізмом автентифікації є пред'явлення користувачем особистого ключа ЕЦП. У цьому випадку ЕЦП використовується як для автентифікації користувача, так і для авторизації доступу до інформації чи ресурсів і таким чином реалізується надійний метод розмежування доступу.

У найбільш узагальненому вигляді процес автентифікації користувача із застосуванням ЕЦП можна подати в такий спосіб. У процесі здійснення доступу користувач вставляє електронний засіб (ЕЗ) у спеціальний пристрій (порт), що підключений до робочої станції, і потім вводить свою ознаку автентифікації (сертифікат відкритого ключа, особистий ключ, біометричну інформацію тощо). Процес автентифікації користувача розпочинається тільки за наявності, у найпростішому випадку, електронного засобу в пристрої зчитування або шляхом порівняння ідентифікатора користувача, уведеного з клавіатури чи іншим способом, з ідентифікатором користувача, що зберігається в ЕЗ. Потім у робочій станції (РС) ознака автентифікації, що введена користувачем, зіставляється з інформацією, що зберігається в ЕЗ. При успішному порівнянні РС надає доступ до інформації та/або своїх ресурсів, і процес автентифікації вважається завершеним (рис. 6.21).

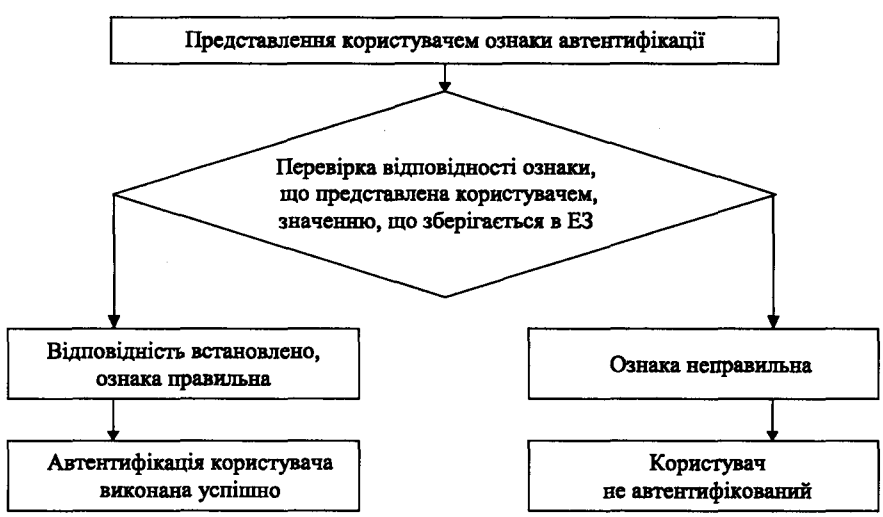

Рис. 6.21. Схема автентифікації користувача

Протоколи автентифікації з використанням пароля користувача добре представлені в [13, 215, 216].

У цьому випадку в ролі ознаки автентифікації користувача виступає особистий пароль користувача. Пароль може зберігатися як у відкритому вигляді, так і в зашифрованому вигляді або у вигляді його геш-значення. В останніх випадках забезпечується суттєва захищеність паролю від його компрометації, у тому числі при втраті ЕЗ. Правильність пароля користувача перевіряється безпосередньо в ЕЗ. При цьому пароль передається в ЕЗ у відкритому вигляді, де відбувається порівняння цього пароля зі збереженим в ЕЗ паролем, попередньо розшифрованим засобами самого ЕЗ. Пароль в ЕЗ завжди зберігається в зашифрованому вигляді, і доступ до нього без знання головного (майстра) ключа ЕЗ практично є неможливим. Але такий протокол автентифікації повинен забезпечувати більш надійне зберігання даних і обробку інформації автентифікації, оскільки втрутитися в процедуру автентифікації, що виконується в ЕЗ, неможливо, на відміну від робочої станції, робота якої завжди може контролюватися, причому навіть порушниками.

При реалізації такого протоколу користувачеві для одержання доступу до інформації чи ресурсів робочої станції необхідно мати ЕЗ із занесеною на нього індивідуальною інформацією про користувача і знати пароль.

У системах з високими вимогами до безпеки, пароль на ЕЗ повинен заноситися адміністратором системи й підписуватись його ключем у процесі виконання процедури персоналізації. Також можливий варіант використання протоколу з третьою довірчою стороною, що виготовить і буде підтримувати сертифікат адміністратора системи.

6.8.2. Автентифікація з використанням ЕЗ та шифрування

Цей метод найчастіше використовується для здійснення автентифікації пред'явника ЕЗ, наприклад, старт-картки чи електронного ключа. Так, перед початком виконання фінансової транзакції, наприклад, з метою зняття грошей з рахунку, оплата покупки тощо, пред'явникові картки пропонується ввести відомий тільки йому особистий (персональний) ідентифікаційний номер – PIN-код (Personal Identification Number). Як правило, число спроб уведення PIN обмежене (не більше 3-х спроб). У випадку, якщо PIN уведений неправильно, картка чи ЕЗ блокується (тимчасово або постійно), а картка може затримуватись терміналом і видається власникові у відділенні банку після засвідчення його особистості. При цьому старт-картка чи електронний ключ зберігають зашифрований PIN-код у системній області EEP ROM, що може бути недоступною.

Розглянемо детальніше автентифікацію з використанням ЕЦП, тобто асиметричного криптографічного перетворення.

Для умов, що розглядаються, ЕЗ повинні забезпечити надійну ідентифікацію та автентифікацію користувача та містити захисну інформацію (наприклад ключі шифрування та сертифікат відкритого ключа), необхідну для безпечної роботи користувача ЕЗ в будь-якому оточенні. Тому в ЕЗ щонайменше повинні використовуватися сертифікати відкритого ключа користувача, особистий ключ для підпису, один або декілька ключів шифрування інформації. Сертифікати відкритих ключів можуть бути виготовлені відповідно до стандартів [6, 13] і обслуговуватись відповідними центрами сертифікації ключів або бути виготовлені за якою-небудь іншою технологією з метою спрощення роботи (наприклад, прості сертифікати, що обмежені до використання тільки всередині своєї організації).

Для заданих умов ЕЗ, наприклад, пластикова картка в мінімальній конфігурації, повинна задовольняти таким вимогам:

1) картка має пам'ять або захищену пам'ять;

2) обсяг доступної пам'яті для даних користувача – 1 кілобайт (8 кілобіт);

3) бажаний захист щодо запису/ читання інформації з картки за допомогою паролю.

Краща конфігурація картки є такою:

1) картка має мікропроцесор (старт-картка);

2) обсяг доступної пам'яті під дані користувача – 2 і більше кілобайт;

3) наявність системи розмежування доступу до даних картки (парольний, ключовий захист, захист за допомогою PIN-коду тощо);

4) можливість зашифрування даних, переданих з картки й розшифрування даних, що одержані від термінала.

6.8.3. Особливості автентифікації із застосуванням сертифікатів відкритих ключів

Протоколи з нульовим розголошенням знань (ISO/IEC 9798-5) здебільшого призначені для здійснення автентифікації користувачів за допомогою різних ЕЗ. При цьому на картку заноситься деяка інформація, що є конфіденційним ключем користувача, наприклад, особистий ключ ЕЦП. Тому конфіденційний ключ є невід'ємною частиною особистості користувача, і якщо користувач доведе знання цього конфіденційного ключа, то автоматично вважається, що користувач довів свою дійсність, тобто здійснив автентифікацію.

Загальна ідея протоколів автентифікації з ЕЦП (з нульовим розголошенням) полягає в тому, що законний користувач, що знає особисте перетворення (ключ) P і відкрите перетворення перевірки (ключ) V, здійснюють спільний криптографічний протокол інтерактивного доказу. У процесі доказу P повинен довести свою справжність, продемонструвавши знання конфіденційного ключа користувача, але не розголосивши його перевірнику V. Це означає, що з інформації, що отримана V, складно обчислити, тобто практично неможливо одержати секретний ключ P.

Усі ці протоколи виконуються в два етапи – попередній етап та робочий, який виконується, як правило, у реальному часі. На попередньому етапі, що виконується заздалегідь, при видачі інтелектуального ЕЗ, наприклад старт-картки, власникові необхідно специфікувати деякі параметри протоколу, і потім формуються необхідні величини, що застосовуються в робочому (реального масштабу) етапі протоколу, зокрема відкриті й особисті (конфіденційні) ключі користувача. На робочому етапі, що здійснюється в процесі виконання транзакції, виконується доказ справжності P.

В основному протоколи автентифікації з нульовим розголошенням призначені для авторизації користувача в деякій системі, наприклад, у системі контролю доступу, але також можуть бути використані для проведення взаємної автентифікації користувачів деякої системи або навіть для проведення взаємної автентифікації користувачів відкритих мереж типу Internet. У цьому випадку необхідна деяка третя сторона, якій будуть довіряти обидва учасники автентифікації, наприклад, центр сертифікації ключів. Цей центр буде формувати асиметричні пари особистий/ відкритий ключі для користувачів, видавати їм особисті ключі

та зберігати відкриті ключі в спеціальній базі даних, до якої може звернутися будь-який користувач із запитом на відкриті ключі іншого користувача для проведення автентифікації.

Приклад протоколу Файне-Фіата-Шаміра [217] з нульовим розголошенням знань наведений нижче в таблиці 6.2. Пересилання повідомлень між учасниками відображені стрілками. Перевірка виконання рівностей (рівнянь) позначена відповідно знаками = ? і ? ?.

Таблиця 6.2. **Протокол Файне-Фіата-Шаміра**

Попередній етап		
P	*V*	Третя довірча сторона
s, v		$n = p\,q$ – випадкове $v \in QR$ $s = \min\{(\sqrt{v^{-1}}^{n}) \bmod n\}$
n, v		

Механізм (протокол) автентифікації		
	P	*V*
1	r – випадкове, $r < n$, $x = r^2 \bmod n$ →	
2	←	$b \in \{0, 1\}$ – випадкове
3	$if(b = 0)$, r $if(b = 1), b = r * s \pmod n$ →	
4		$if(b = 0)\ x = ?\ r^2 \pmod n$ (чи знає $P\ \sqrt{x}$?); $if(b = 1)\ x = ?\ y^2 v \pmod n$ (чи знає $P\ \sqrt{v^{-1}}$?)

Стійкість протоколу Файне-Фіата-Шаміра заснована на складності добування квадратного кореня за модулем та коли невідоме розкладання n на множники.

Протокол Файне-Фіата-Шаміра не є оптимальним для реалізації на ЕЗ, головним чином, через велику кількість обмінів між ЕЗ і пристроєм доступу й обсягу даних, які необхідно зберігати в кожній ітерації. На практиці, при реалізації в СЗІ від НСД, замість протоколів автентифікації з нульовим рівнем розголошення знань, використовують альтернативні протоколи Guillou-Quisquater або протокол Шнорра (Schnorr) і засновані на них похідні протоколи.

Необхідно відзначити, що всі протоколи автентифікації, засновані на асиметричних алгоритмах, мають одну цікаву властивість – вони стандартним чином можуть бути перетворені на схеми цифрового підпису [7, 9, 10, 210].

6.8.4. Особливості біометричних методів автентифікації

Біометричні пристрої автентифікації існують уже близько двадцяти п'яти років. За цей час вони зі шпигунських фільмів перемістилися на робочі столи й істотно подешевшали. На ринку є безліч систем з біоідентифікацією вартістю від декількох десятків до декількох мільйонів доларів. З їхньою допомогою можна захистити й окремий ПК, і корпоративну мережу. Останні дослідження показали, що біометричні методи можуть ефективно застосовуватись сумісно з асиметричними криптографічними перетвореннями, перш за все ЕЦП.

До широкого впровадження цих систем готується й Microsoft, що оголосила про плани вбудовування у Windows механізмів захисту на основі біометричних технологій, коли персональний комп'ютер буде узнавати свого хазяїна за відбитками пальців, голосом, райдужною оболонкою ока тощо [218].

Біоідентифікація заснована на унікальності характеристик людського тіла. Вважається, що не існує двох людей з однаковими біометричними ознаками.

Біометрія (Biometrics) – це прикладна область знань, що використовує при створенні різних автоматичних систем розмежування доступу унікальні ознаки, властиві кожній окремій людині. До цих ознак, які називають біометричними характеристиками (Biometric Parameters), належать:

- папілярний візерунок пальця;
- форма кисті руки;
- візерунок райдужної оболонки ока;
- параметри голосу;
- риси особи;
- термограми особи (наприклад схема кровоносних судин);
- форма й спосіб підпису;
- фрагменти генетичного коду тощо.

Потрібно розрізняти біометричну характеристику та біометричний зразок (Biometric Sample), тобто спостереження обраної біометричної характеристики. Більшість біометричних систем функціонує в такий спосіб. У базі даних системи безпеки зберігається цифровий образ відбитка пальця, райдужної оболонки ока або голосу. Людина, що одержує доступ до ЕЗ, за допомогою мікрофона, сканера чи інших пристроїв уводить в систему свій біометричний зразок. Система витягає з нього дані (особливі точки та їхні параметри), порівнює їх з тими, що зберігаються в БД, визначає ступінь збігу й робить висновок про те, чи вдалося ідентифікувати людину за пред'явленими даними, а також підтвердити, що вона саме та, за кого себе видає.

Аналіз показує, що ринок біометрії інтенсивно зростає. Серед корпорацій з ринковою вартістю більше 5 млрд дол. у лідери вийшла Symantec. Різко підвищилися акції компаній, що спеціалізуються на зберіганні даних (Network Appliance і Veritas Software). Цей вид бізнесу став актуальним після втрати величезного банку даних у Всесвітньому торговому центрі в результаті теракту.

Розвиток ринку біометрії значною мірою є результатом останніх подій. І хоча тенденції до росту позначилися тут ще за рік до терактів, останні радикально змінили технологічні пріоритети. Серед громадян США до 10 вересня 2001 р. усього 10 % підтримувало ідею біометричної паспортизації та більше 75 % – після.

Світовий ринок біометричних систем сьогодні представлений десятками відомих фірм (а всього на ньому більш ніж 300 компаній займаються продажем, розробкою й обслуговуванням систем).

IDC протягом двох років (з 2000 по 2001 роки) ретельно вивчала світовий ринок біометрії, виявляючи його тенденції та реальні зміни, і в жовтні 2002 року опублікувала звіт Worldwide Hardware and Biometrics Authentication Forecast and Analysis.

Структура ринку біометричної автентифікації й ідентифікації виглядає так:

– верифікація голосу – 11 %;
– розпізнавання особи – 15 %;
– сканування райдужної оболонки ока – 34 %;
– сканування відбитків пальців – 34 %;
– геометрія руки – 25 %;
– верифікація підпису – 3 %.

За оцінками, його обсяг до 2003 року склав 1 млрд доларів, а на 2005 рік перевищує 5 млрд дол. Майже 50 % біометричних систем доводиться на частку дактилоскопії.

Згідно зі статистичними даними, річний темп розвитку біометрії – 40 %. Це досить високий показник навіть для зростаючої економіки, а на тлі загального спаду у сфері високих технологій біометрія виглядає особливо перспективно. При збереженні таких темпів через 10–15 років населення Землі буде забезпечено біометричними посвідченнями особи, інформація про які буде зберігатися в державних базах даних, об'єднаних у глобальну міжнародну ідентифікаційну систему. Однак, на думку експертів, зараз ми переживаємо пік інтересу до біометрії, і після 2010 року нам варто очікувати спокійнішої ринкової динаміки.

На американському ринку в галузі систем верифікації підписів лідирують компанії Cyber-Sign і Communications Intelligence, Identix, Sagem Morpho, Veridicom і Infineon, які намагаються прибрати до рук ринок сканерів відбитків пальців. І, нарешті, аутентифікацією голосу займаються T-Netix, ITT Nuance і Veritel. Є й сотні дрібніших фірм.

Деякі аналітики, що вивчають ринок технологій автентифікації, стримано оцінюють практичні можливості біометричних пристроїв. Наприклад, Білл Кэмпбелл, консультант компанії Eagle's Reach, що спеціалізується на захисті інформації, вважає: «Біометрія схожа на процес упізнавання при очній ставці. Системам, що функціонують подібним чином, властиві помилкові спрацьовування, що визнають й самі виробники. Питання й у тім, чи припустимі в принципі помилкові спрацьовування біометрії в критично важливих системах. Один з можливих шляхів зниження їхньої частки – одночасна перевірка декількох параметрів, наприклад, і голосу, і відбитків пальців».

Поки не існує єдиної системи тестів для оцінки «рівноймовірності помилок» (характеристика, якою прийнято позначати точність біометричних систем). Це не дозволяє порівнювати за ефективністю методики різних виробників.

Однак, принаймні чотири біометричних методи довели свою практичність: розпізнавання за відбитками пальців, райдужною оболонкою, сітківкою ока та рисами обличчя.

Розпізнавання за відбитками пальців

Відбиток пальця утворює так звані папілярні лінії на гребішкових виступах шкіри, розділених борозенками. Із цих ліній складаються складні візерунки (дугові, петлі й виткові), які мають такі властивості:

– індивідуальність і неповторність;

– стійкість (від внутрішньоутробного розвитку й до розкладання трупа);

– відновлюваність (при поверхневому порушенні шкіри рисунок ліній відновлюється в колишньому вигляді).

Усе це дозволяє абсолютно надійно ідентифікувати особистість.

Із усього різноманіття продукції, представленої на світовому ринку біометричних систем ідентифікації, найбільшою популярністю користуються автоматичні системи розпізнавання відбитків пальців – AFIS [218]. У примусовому порядку AFIS використається для збору відбитків пальців у криміналістиці, найчастіше для поліцейської дактилоскопії.

На частку AFIS доводиться половина обсягу продажів біометричної продукції, а з урахуванням криміналістичних систем – 80 %. Сканування відбитка пальця – найстаріший метод з усіх існуючих у біометрії й при цьому один із найперспективніших.

Пристрої сканування відбитків пальців прості й зручні в застосуванні: досить доторкнутися до сканера. Так, розробка BioLink Technologies дозволяє за 0,1 с зняти відбиток пальця, за 0,2 с розпізнати його й дозволити доступ до інформації. На відмінність від систем сканування сітківки ока, зняття відбитків пальця за допомогою AFIS не викликає дискомфорту в користувачів. Відбиток пальця індивідуальний і не міняється згодом. Системи розпізнавання за відбитками пальців демонструють високі показники точності: імовірність того, що доступ до конфіденційних відомостей одержить неавторизований користувач, практично дорівнює нулю.

Комерційні AFIS-системи забезпечують малі значення відмови (помилкової відмови) в доступі (False Reject Rate, FRR) при деякому заданому коефіцієнті пропуску (False Accept Rate, FAR). Для FRR – це ймовірність того, що система не буде визнавати дійсність відбитка пальця зареєстрованого користувача, а FAR – імовірність того, що система помилково визнає дійсність відбитка пальця користувача, не зареєстрованого в системі.

Постачальники зазвичай заявляють значення FRR близько 0,01 %, а FAR – 0,001 %. Значення, при якому ці показники дорівнюють одне одному, називається рівною нормою помилки й часто приймається близько 0,1 %. Зараз активно розробляються алгоритми, стійкі до шуму в зображеннях – образах відбитка пальця, що дозволяє домогтися збільшення точності й швидкості розпізнавання в реальному часі.

Завдяки економічності та малим розмірам, пристрої сканування можуть бути інтегровані в комп'ютерну мишу, клавіатуру або ноутбук. Зараз їхня вартість становить близько 100 дол. Серед біометричних систем автентифікації сканери відбитків пальців найдешевші й тому є найуразливішими пристроями. Система, що використовує відбитки пальців, може бути обманута восковою фігурою з раніше викраденим зразком відбитка пальців [218]. Таке злодійство цілком можливе.

Японський фахівець з безпеки Цутомі Мацумото на практиці показав, як просто обдурити біометричні сканери відбитків пальців. Підроблений палець, створений їм із желатину й пластикового шаблона, успішно проходив через сканер у чотирьох випадках із п'яти. Більш того, якщо нечіткий відбиток перенести на скло, то його можна поліпшити за допомогою ціанокоболаміна (вітамін B12), тонкого шару будь-якого суперклею й цифрової камери. Пакет PhotoShop дозволяє підвищити контрастність зображення й перенести отриманий результат на плівку. Цутомі Мацумото перевірив 12 різних комерційних сканерів відбитків пальців і на всіх продемонстрував 80 %-ву можливість такого злому.

6.9. ОСНОВНІ ХАРАКТЕРИСТИКИ ТА РЕАЛЬНІ КЛАСИ ЩОДО КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ АВТЕНТИФІКАЦІЇ З ЕЦП

Згідно загальних вимог кожному процесу інформаційної взаємодії між об'єктами (процесами) повинні передувати протоколи односторонньої або двосторонньої автентифікації, встановлення ключів, узгодження та підтвердження ключів, явної чи неявної автентифікації ключів тощо.

6.9.1. Основні характеристики криптографічних протоколів на основі ЕЦП

За результатами аналізу й порівняння різних криптографічних протоколів визначено необхідність урахування при виборі криптографічних протоколів таких потенційних послуг, характеристик і властивостей [7, 10, 51, 210, 213]:

1) наявність (реалізація) послуги автентифікації об'єкта (процесу), суб'єкта;
2) наявність (реалізація) послуги автентифікації ключа (ключів);
3) вид автентифікації об'єктів (процесів) і суб'єктів;
4) вид автентифікації ключів;
5) наявність послуги встановлення ключа (ключів);
6) наявність послуги підтвердження ключа (ключів);
7) новизна ключа (ключів) на кожному з етапів встановлення ключів;
8) перелік послуг з управління ключами;
9) захищеність від загроз типу «передача раніше переданого легального повідомлення», типу «Повтор»;
10) захищеність від загроз типу «Маскарад»;
11) захищеність від загроз типу «Модифікація»;
12) криптографічна живучість у встановлених ключів;
13) гарантії забезпечення послуг, конфіденційність, цілісність, доступність, справжність (автентичність) і неспростовність щодо інформації автентифікації та ключів;
14) число обмінів при здійсненні криптографічного протоколу;
15) складність виконання криптоаналізу відносно ключів та захищуваної інформації;
16) складність обчислень при здійсненні криптографічного протоколу;
17) можливість виконання попередніх обчислень;
18) наявність та вимоги до третьої довірчої сторони тощо.

6.9.2. Аналіз класів механізмів і криптографічних протоколів автентифікації

Аналіз ряду джерел [7, 10, 51, 210] показав, що механізми та їх конкретна реалізація у вигляді криптографічних протоколів автентифікації можуть піддаватися атакам, які обмежують їх ефективність.

Будь-які механізми автентифікації, які можна використовувати для надання підтримки у фазі передавання, класифікують відносно загроз(и), проти яких ці механізми є невразливими. Усі розглянуті механізми можна застосовувати до об'єктів автентифікації, а механізми з цифровим підписом (геш-значенням) також можна застосовувати до автентифікації даних.

6.9.2.1. Практичні класи механізмів автентифікації

Розглянемо практичні аспекти реалізації механізмів і на їх основі криптографічних протоколів автентифікації. Будемо згідно з [210] основні класи механізмів автентифікації за рівнем захищеності від загроз визначати таким чином:

Клас 0	Незахищений
Клас 1	Захищений від розкриття заявленої інформації автентифікації (ІА)
Клас 2	Захищений від розкриття заявленої ІА та атаки типу «Повтор» для різних перевірників
Клас 3	Захищений від розкриття заявленої ІА та атаки типу «Повтор» на одного перевірника
Клас 4	Захищений від розкриття заявленої ІА та атаки типу «Повтор» на одного перевірника чи різних перевірників

Проведемо аналіз захищеності практичних механізмів. Так, у механізмах автентифікації класу 1 надається захист від розкриття заявленої ІА. Ці механізми можуть застосовуватися для автентифікації джерела даних та об'єкта. Механізми ґрунтуються на використанні функції перетворення, при цьому заявлена ІА може бути комбінована з розпізнавальним ідентифікатором та перетворюється за допомогою цієї функції перетворення. Значення, що отримуємо, передається разом з розпізнавальним ідентифікатором, а відкрите значення заявленої інформації не передається по комунікаційному каналу.

Як приклади механізмів цього класу можна привести такі:

– передача паролю у вигляді криптографічного контрольного значення або геш-значення;

– передача цифрового відбитку, зашифрованого на таємному ключі;

– передача паролю, зашифрованого на таємному ключі;

– передача цифрового відбитку, підписаного з використанням особистого ключа.

Таким чином, механізми автентифікації класу 1 уразливі проти атаки типу «Повтор», наприклад, пароль, що передається, можна знов відтворювати на рівні протоколу обміну, але відкритий пароль, який використовується на рівні системного інтерфейсу, не розкривається.

Функції перетворення $F()$, що використовуються для одержання обмінної ІА, повинні задовольняти таким вимогам:

1) у разі однонаправленої функції забезпечується захист від розкриття заявленої ІА (ЗРІА) При перевірці знову використовують однонаправлену функцію та перевірочну ІА замість заявленої ІА та порівнюють з одержаною обмінною ІА;

2) у разі використання симетричного шифрування для забезпечення ЗРІА при перевірці використовується перевірочна ІА та інформація, отримана в результаті розшифрування одержаної обмінної ІА, а потім порівнянням перевіряється справжність розшифрованих даних. Це здійснюють шляхом перевірки збігу розшифрованого розпізнавального ідентифікатора та розпізнавального ідентифікатора пред'явника, правильністю цифрового відбитку та паролю тощо;

3) у разі цифрового підпису перевірка здійснюється шляхом обчислення цифрового відбитку від одержаних даних. Для перевірки того, що одержаний підпис є дійсним підписом для даного відбитку, використовується перевірочна ІА;

4) додатково, у разі автентифікації джерела даних, цифровий відбиток, який одержано з обмінної ІА, порівнюють з регенерованим цифровим відбитком даних, необхідних для автентифікації;

5) у разі необхідності надання конфіденційності функція перетворення повинна бути однонаправленою або мати експоненційну складність зворотного перетворення для тих, що не повинні мати доступ до конфіденційної заявленої ІА (цифрового відбитку).

При застосуванні механізмів класу 2 забезпечується захист від розкриття заявленої ІА та атаки типу «Повтор» на різних перевірників. Цей клас механізмів автентифікації забезпечує захист від розкриття заявленої ІА та атак типу «Повтор» на різних перевірників, але не забезпечує захист від атак типу «Повтор» з однаковим перевірником. Цей клас механізмів захисту ідентичний класу 1, але додатково на вхід функції перетворення подається унікальна характеристика обраного перевірника, що забезпечує додатковий захист.

При застосуванні механізмів класу 3 забезпечується захист від розкриття заявленої ІА та атаки типу «Повтор» на одного перевірника.

Унікальні механізми цього класу використовують функції перетворення разом з унікальною інформацією для надання додаткового захисту від атаки типу «Повтор» на одного перевірника. Заявлена ІА та унікальний номер перетворюються і передаються разом із розпізнавальним ідентифікатором.

Дані щодо унікального числа можуть бути подані таким чином:

– *випадкове* або *псевдовипадкове число* – число, яке не може навмисне бути повторене упродовж життєвого циклу заявленої ІА, причому випадкове або псевдовипадкове число з достатньо великого ряду може знизити ймовірність того, що таке число вже використовувалося;

– *позначки (мітки) часу* – мітка часу є унікальним числом упродовж життєвого циклу заявленої ІА, що одержано з довірчого джерела, причому старі мітки часу, або попередньо використані мітки часу, будуть видалені;

– *лічильник* – значенням лічильника є унікальне число, яке постійно збільшується, доки використовують однакову заявлену ІА.

– *криптографічне зв'язування* – унікальне число є значенням, одержаним зі змісту попередніх даних, що передаються між пред'явником і перевірником шляхом витягу в деякий момент часу. Унікальність цього числа може гарантуватися пред'явником за рахунок конкатенації його з даними, що є унікальними для пред'явника, наприклад такими, як особистий розпізнавальний ідентифікатор пред'явника.

– комбінація наведених вище методів для створення унікального числа.

Як функція перетворення можуть бути використані:

– *однонаправлена функція* – унікальне число, заявлена ІА та, можливо, розпізнавальний ідентифікатор перетворюються за допомогою однонаправленої функції. Унікальне число також передається перевірнику, тому він може виконати таке саме перетворення;

– *асиметричний алгоритм* – заявлена ІА є особистим ключем, при цьому унікальне число підписується на особистому ключі;

– *симетричний ключ* – заявлена ІА є таємним ключем, при цьому унікальне число зашифровується на таємному ключі.

Цей клас механізмів застосовується для автентифікації джерела даних та об'єкта. Унікальне число генерується за допомогою ЗРІА, а потім виконується зашифрування також і таких вхідних даних [210]:

– унікальне число;

– заявлена ІА;

– розпізнавальний ідентифікатор (необов'язково);

– цифровий відбиток (у разі автентифікації джерела даних).

При перевірці розшифровують та перевіряють дійсність обмінної ІА, використовуючи перевірочну ІА, а також перевіряють унікальність одержаного унікального числа. Якщо таке число вже було одержано раніше, то видається повідомлення про повторення унікального числа. При використанні послуги автентифікації джерела даних додатково порівнюється цифровий відбиток з обмінної ІА та цифровий відбиток, що виробляється з одержаних даних.

У класі 4 забезпечується захист від розкриття заявленої ІА та атак типу «Повтор» на одного перевірника та різних перевірників. У класі 4 введено ще чотири проміжні класи – 4*a*, 4*b*, 4*c*, 4*d*.

1. Проміжний клас 4*a* називають механізмом з унікальним числом.

Клас 4*a* ідентичний класу 3, але для надання додаткового захисту на вхід функції перетворення подається унікальна характеристика обраного перевірника.

2. Проміжний клас 4*b* називають механізмом із запитом паролю.

У класі 4*b* гарантується захист від атак типу «Повтор», тобто будь-яка спроба зробити автентифікацію себе шляхом повтору обмінної ІА закінчиться невдало. Реалізується цей захист таким чином. Пред'явник формує запит на автентифікацію. У відповідь перевірник формує запит пред'явнику на перевірку паролю у формі елемента даних з унікальним значенням. Пред'явник перетворює інформацію запиту на перевірку пароля та заявлену ІА за допомогою деякої функції. Результуюче значення цієї функції відсилається перевірнику.

Таким чином, у механізмі класу 4*b* із запитом паролю використовують трьохпрохідний протокол обміну інформацією, який включає:

а) відправку запиту на автентифікацію від пред'явника перевірнику;

б) генерування перевірником запиту на перевірку пароля та передачу його пред'явнику;

в) обчислення пред'явником за допомогою деякої визначеної функції F відповіді від заявленої ІА, можливо комбінованої з розпізнавальним ідентифікатором, та інформації запиту на перевірку паролю.

У загальному випадку розпізнавальний ідентифікатор може відсилатися або в запиті на автентифікацію, або з кінцевою відповіддю.

Як функція перетворення F у класі 4*b* можуть бути використані:

– однонаправлена функція, за допомогою якої запит на перевірку паролю та обмінна ІА перетворюються;

– асиметричний алгоритм, коли заявлена ІА є особистим ключем, при цьому запит на перевірку пароля підписується на особистому ключі;

– симетричний алгоритм, коли заявлена ІА є таємним ключем, при цьому запит на перевірку паролю зашифровують на таємному ключі.

Особливістю механізмів із запитом паролю є те, що генерування запиту на перевірку пароля залежить від ідентифікаційних даних, одержаних у запиті на автентифікацію. У цьому випадку розпізнавальний ідентифікатор обов'язково присутній у запиті на автентифікацію, при цьому може використовуватись ще четверта функція перетворення – некриптографічний алгоритм. Прикладом є використовування таблиці з парами одержаних запитів на перевірку паролю. Іншими прикладами є біометричні схеми, перш за все, засоби повтору голосу.

Цей проміжний клас використовується для автентифікації джерела даних та об'єктів.

3. У проміжному класі 4*c* використовуються спеціалізовані механізми із запитом паролю та шифруванням. У спеціалізованих механізмах із запитом паролю та шифруванням використовують трьохпрохідну передачу інформації. Сутність етапів полягає в такому:

а) відправка пред'явником запиту на автентифікацію з використанням розпізнавального ідентифікатора;

б) генерація перевірником запиту на перевірку пароля з використаннням перевірочної інформації ІА, можливо, разом з розпізнавальним ідентифікатором, та подальше перетворення її за допомогою деякої відповідної функції F;

в) відправка пред'явником відповіді, що містить інформацію запиту на перевірку паролю.

Механізми із запитом паролю та шифруванням ґрунтуються на використанні:

– асиметричного алгоритму, коли заявлена ІА є особистим ключем, при цьому запит на перевірку паролю зашифровується на відповідному відкритому ключі;

– симетричного алгоритму, коли заявлена ІА є таємним ключем, при цьому запит на перевірку паролю зашифровується на таємному ключі.

Цей проміжний клас 4*c* використовується для гарантованої автентифікації джерела даних та об'єктів. У проміжному класі 4*d* використовуються механізми з обчисленням відповіді. Відповідні протоколи реалізуються за три проходи у такій послідовності:

1) формування та відправка запиту на автентифікацію з використанням деяких значень та інформації відносно ідентифікаційних даних;

2) генерування запиту на перевірку пароля, який показує, яке значення обрано перевірником;

3) відправка відповіді, що містить перетворене за допомогою деякої визначеної функції унікальне число, запит на перевірку паролю або обрані значення для обчислення відповіді та заявлену ІА.

Для надання більших гарантій ідентифікаційним даним обміни можуть повторюватися декілька разів. Такий механізм забезпечує захист від атак типу «Маскарад». При цьому порушник може обчислити коректну відповідь тільки для деяких значень, але не для всіх, які може обрати перевірник. При використанні тільки одного обміну перевірник може обрати значення, для якого порушник знає коректну відповідь. При збільшенні числа обмінів зменшується ймовірність успішного виконання такої атаки.

У процесі виконання трьох етапів здійснюється:

– формування пред'явником запиту на автентифікацію, який включає розпізнавальний ідентифікатор, унікальне число та вибір значень;

– формування перевірником запиту на перевірку паролю з обраними значеннями;

– формування пред'явником захищеного запиту на перевірку паролю.

Процес здійснення декількох запитів відповідей повторюється необхідне число разів.

Аналіз показав, що особливу групу складають класи механізмів автентифікації, у яких ініціатором запиту є перевірник. Відповідні механізми описані у [210]. Вони можуть застосовуватися для випадків, коли як ініціатор обмінів при автентифікації виступає перевірник. При цьому кількість етапів передавань зміниться.

При здійсненні автентифікації повинна враховуватись специфіка використання сертифікатів автентифікації. Сутність її у такому. По-перше, механізми автентифікації можуть реалізовуватись з використанням перевірочної ІА у вигляді інтерактивних або автономних сертифікатів автентифікації. По-друге, перевірочна ІА, яка надається додатковим шляхом, наприклад, з використанням захищених каналів зв'язку. По-третє, інтерактивний сертифікат автентифікації може використовуватися для надання доказу автентифікації, використовуючи принципи, що наведені в [210]. При цьому сертифікат автентифікації служить доказом того, що ТДС здійснила зв'язок між даним розпізнавальним ідентифікатором та спеціалізованою перевірочною ІА, наприклад, відкритим ключем.

6.9.2.2. Особливості здійснення протоколів взаємної автентифікації

Аналіз даних [210] дозволяє зробити висновок, що для проміжних класів механізмів, які залучаються до однопрохідного обміну (проміжні класи 1, 2, 3 та 4*a*), для забезпечення взаємної автентифікації необхідно використовувати однакові формати повідомлень у кожному з двох напрямків.

При цьому для проміжного класу 4*b* однаковий тип механізму можна використовувати в обох напрямках, тобто перший запит на перевірку пароля може надсилатися разом із запитом на автентифікацію, а перетворення першого запиту на перевірку пароля надсилається разом з другим запитом на перевірку пароля. У цьому проміжному класі механізмів в кожному з двох напрямів необхідно здійснювати однакове число обмінів, як для звичайної направленої автентифікації.

Для проміжного класу 4*c* перетворення першого запиту на перевірку пароля може надсилатися разом із запитом на автентифікацію, а перетворення другого запиту на перевірку пароля може надсилатися з першим запитом на перевірку пароля.

Також проміжний клас 4*b* може використовуватися разом із механізмами класу 4*c*. Два запити на перевірку пароля вміщаються разом з даними на передачу. У випадку симетричного шифрування заявлена ІА та перевірочна ІА є однаковими, а перетворення виконується тільки один раз. У випадку асиметричного шифрування виконуються два перетворення окремо для перевірочної ІА та заявленої ІА.

Для реалізації направленої автентифікації у проміжному класі 4*d* необхідно не менше трьох обмінів, у той час як для взаємної автентифікації потрібно щонайменше чотири передавання. Порядок передавання розпізнавальних ідентифікаторів у цій моделі узгоджується згідно з проміжними класами.

6.9.3. Загальна характеристика класів захищеності

У табл. 6.3 представлено результати аналізу вразливості та характеристики різних класів і проміжних класів механізмів, розглянутих вище. Розгляд ґрунтується на [210].

За необхідності об'єкти можуть здійснити автентифікацію із залученням щонайменше однієї ТДС. У цьому випадку необхідно визначити реальну довіру між кожним об'єктом та будь-якою ТДС. У такій моделі залучають тільки одну довірчу сторону, причому ТДС може бути розподіленою в просторі. Інші моделі визначають множину третіх ТДС, які довіряють одна одній, причому в загальній моделі залучається множина ТДС, у якій немає довіри одна до одної. Залучення декількох ТДС може бути обґрунтованим, якщо необхідно забезпечити резервування послуг третьої довірчої сторони.

Таблиця 6.3. **Характеристики класів і проміжних класів механізмів автентифікації**

Проміжний клас уразливості	0	1	2	3	4a	4b	4c	4d
Розкриття заявленої ІА	Т	Н	Н	Н	Н	Н	Н	Н
Атака типу «Повтор» на різних перевірників	Т	Т	Н	Т	Н	Н	Н	Н
Атака типу «Повтор» на одного перевірника	Т	Т	Т	Н	Н	Н	Н	Н
Атака типу «Підміна» з порушником-ініціатором	Н	Н	Н	Н	Н	Н	Н	Н
Атака типу «Підміна», у якій порушник відповідає	Т	Н	Н	Н	Н	Н	Н	Н
Характеристики:								
– симетричні / асиметричні	Сим	Будь-яке	Будь-яке	Будь-яке	Будь-яке	Будь-яке	Будь-яке	Асим
– криптографічні (Т)/ некриптографічні (Н)	Н	Будь-яке	Будь-яке	Будь-яке	Будь-яке	Будь-яке	Т	Т
Кількість передавань								
– пред'явник-ініціатор	1	1	1	1	1	3	3	3
– перевірник-ініціатор	2	2	2	2	2	2	4	4
Надання автентифікації джерела даних	Т	Т	Т	Т	Т	Т	Н	Т

Примітка

У таблиці 6.3 позначення «Т» означає «Так», а позначення «Н» означає «Ні».

6.10. КРИПТОГРАФІЧНІ ПРОТОКОЛИ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ І РОБОЧИХ СТАНЦІЙ НА ОСНОВІ ЕЦП

Для надійної автентифікації користувачів та робочих станцій переважно рекомендується використовувати у користувачів електронні засоби, що спроможні апаратно реалізовувати криптографічні функції. Серед них основними є генерування ключів на основі апаратних засобів, зберігання ключів в електронних засобах з високим рівнем захищеності їх від компрометації, застосування особистих і таємних ключів з високим захистом їх від несанкціонованого доступу, можливість генерування ключів сенсів зв'язку тощо. При цьому в робочих станціях можуть застосовуватись як аналогічні апаратні та апаратно-програмні, так і програмні засоби криптографічних перетворень. Але при встановленні електронних ключів з метою доступу до робочої станції обов'язково необхідно виконати протокол автентифікації та в більшості випадків встановлення (узгодження, підтвердження тощо) ключів.

У цьому розділі наведено та проаналізовано криптографічні протоколи автентифікації РС і користувачів з електронним ключем та встановлення ключів. Як базові вибрані криптографічні механізми і на їх основі протоколи, що містяться в ДСТУ ISO/IEC 9798-3 [213], ДСТУ ISO/IEC 15946-3 [37] та ДСТУ ISO/IEC 11770-3 [22]. На основі аналізу й порівняння механізмів та криптографічних протоколів, що містяться у вказаних стандартах, вироблено рекомендації щодо вибору й застосування криптографічних протоколів з метою автентифікації РС і користувачів з електронним ключем та встановлення ключів. Обґрунтування та аналіз криптографічних протоколів у подальшому будемо вести, спираючись на структурні схеми, що наведені у параграфі 6.4.

6.10.1. Криптографічні протоколи автентифікації користувачів і робочих станцій згідно з ДСТУ ISO/IEC 9798-3

У стандарті ДСТУ ISO/IEC 9798-3 описано механізми та на їх основі криптографічні протоколи автентифікації об'єктів, що ґрунтуються на використанні асиметричних алгоритмів цифрового підпису. Ці механізми та протоколи забезпечують автентифікацію та, за необхідності, встановлення ключів, з рівнем захищеності, що відповідає 4 класу. Перші два механізми визначають автентифікацію одного об'єкта (однобічна автентифікація), а решта механізмів призначена для здійснення взаємної автентифікації двох об'єктів. При цьому для здійснення однобічної автентифікації розглядаються однопрохідний та двопрохідний механізми, а для здійснення взаємної автентифікації розглядаються двопрохідний, трьохпрохідний і паралельний двопрохідний механізми. На основі цих механізмів розроблені криптографічні протоколи, реалізація яких не залежить, по суті, від виду асиметричного перетворення – у кільці, полі Галуа чи групі точок еліптичних кривих, чи навіть зі спарюванням точок еліптичних кривих.

У групі асиметричних перетворень, що подані в стандарті ДСТУ ISO/IEC 9798-3, для доказу ідентифікаційних даних пред'явника, що передаються перевірнику, використовуються алгоритми асиметричних цифрових підписів. При цьому пред'явник формує цифровий підпис, використовуючи свій особистий ключ від

заявлених даних, розпізнавальний ідентифікатор, унікальні числа та унікальні характеристики перевірника. Перевірник одержує цифровий підпис разом з деякими даними, одержує сертифікат відкритого ключа або від пред'явника, або від уповноваженого на розподіл сертифікатів та перевіряє цифровий підпис, використовуючи як вхідні дані перевірочну інформацію, розпізнавальний ідентифікатор та інші дані, необхідні для перевірки цифрового підпису.

Щодо об'єктів автентифікації та механізмів автентифікації у стандарті ISO/IEC 9798-3 визначені такі вимоги. Під час проходження автентифікації об'єкт підтверджує свою ідентичність шляхом пред'явлення доказу того, що він володіє знанням свого особистого ключа цифрового підпису, формуючи за допомогою нього цифровий підпис від певних даних. Причому цифровий підпис може бути перевірений будь-яким об'єктом, який має доступ до відкритого ключа (сертифіката) електронного цифрового підпису.

Основні вимоги, що висуваються до механізмів автентифікації, такі:

1) перевірник повинен володіти дійсним відкритим ключем пред'явника, наприклад, відкритим ключем об'єкта, за який себе видає пред'явник;

2) також ніхто, крім пред'явника, не повинен використовувати та/або знати його особистий ключ.

Наведені вимоги мають бути виконаними, інакше це може призвести до виникнення загрози компрометації процесу автентифікації або навіть до неможливості його успішного виконання.

Аналіз підтверджує [13, 15, 16, 21, 113], що найбільш поширеним шляхом отримання дійсного відкритого ключа є використання сертифіката відкритого ключа, який може пересилатися пред'явником разом з обмінною ІА, або одержуватися від уповноваженого на розподіл сертифікатів. Від систем типу «інфраструктура відкритих ключів» (ІВК) можна одержувати сертифікати, а також перевіряти для уникнення можливості автентифікації об'єктів з компрометованими особистими ключами статус сертифіката.

Також у подальшому, у зв'язку з тим, що широкого застосування набули стандартизовані електронні цифрові підписи з додатком (доповненням), ми будемо аналізувати тільки механізми та протоколи автентифікації, що ґрунтуються на ЕЦП з додатком.

З урахуванням вимог до взаємної автентифікації користувача, що використовує електронний ключ, і робочої станції, як базовий краще вибрати трьохпрохідний протокол автентифікації та встановлення ключа ДСТУ ISO/IEC 9798-3. При цьому ініціатором автентифікації (пред'явником), як правило, є користувач з електронним ключем. Встановлений ключ, як правило, призначений для автентифікації та створення для обміну інформацією між об'єктами криптотунелів. У такому випадку криптотунель встановлюється між електронним ключем та РС користувача (безпосередньо модулем захисту РС). Цей механізм автентифікації виконується за три проходи та два кроки і ґрунтується на двопрохідному механізмі однобічної автентифікації, що наведено в ДСТУ ISO/IEC 9798-3. У подальшому розгляд будемо вести в узагальненому вигляді, тобто проведемо аналіз самого механізму. Також будемо вважати, що цей криптографічний механізм стає криптографічним протоколом при конкретному виборі й фіксації стандарту цифрового підпису та функції вироблення ключа для криптотунелю. Але, незважаючи на

вказане, відразу зафіксуємо, що як стандарт ЕЦП, якщо це не оговорено окремо, повинен використовуватись національний стандарт ДСТУ 4145-2002. За інших умов будемо оговорювати це окремо.

У механізмі автентифікації, що аналізується, процес взаємного проходження автентифікації ініціює користувач B, що має електронний ключ (рис. 6.22). Стороною A є РС (модуль захисту).

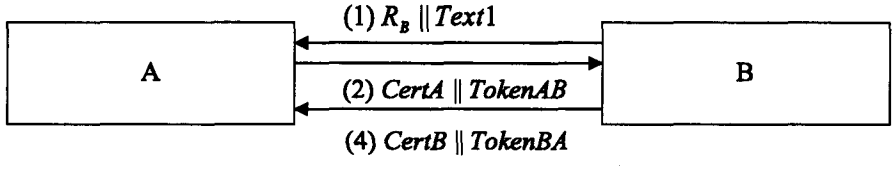

Рис. 6.22. Взаємна автентифікація з трьома проходами

При формуванні запиту на автентифікацію та встановлення ключа, електронний ключ формує запит у вигляді $R_B \mid Text1$, де R_B – пароль запиту (випадкове число), а $Text1$ – текстове повідомлення.

Форми маркерів мають вигляд:

$$TokenAB = R_A \| R_B \| B \| Text3 \| sS_A(R_A \| R_B \| B \| Text2), \quad (6.16)$$

$$TokenBA = R_B \| R_A \| A \| Text5 \| sS_B(R_B \| R_A \| A \| Text4). \quad (6.17)$$

Для формування маркера $TokenAB$ об'єкт A використовує запит на перевірку пароля R_B об'єкта B, свій запит на перевірку пароля R_A, розпізнавальний ідентифікатор B разом із формуванням підпису $sS_A(R_A \| R_B \| B \| Text2)$ від заявлених даних $Text2$ та значень R_A, R_B, розпізнавального ідентифікатора B. Для формування маркера $TokenBA$ об'єкт B використовує запит на перевірку пароля R_B, що був відісланий на першому проході, запит на перевірку пароля R_A об'єкта A, що одержано з маркера $TokenAB$, розпізнавальний ідентифікатор A разом з формуванням підпису $sS_B(R_B \| R_A \| A \| Text4)$ від заявлених даних $Text4$ та значень R_A, R_B розпізнавального ідентифікатора A.

Механізм, що наведено на рис. 6.22, покроково описується таким чином:

1. Об'єкт B генерує випадкове число R_B та надсилає його об'єкту A (також об'єкту A може бути надіслане текстове поле $Text1$).

2. Об'єкт A генерує та надсилає маркер $TokenAB$ об'єкту B, а також (необов'язково) свій сертифікат.

3. Після отримання повідомлення, що містить $TokenAB$, об'єкт B виконує такі кроки:

а) впевнюється в тому, що володіє дійсним відкритим ключем об'єкта A, за допомогою або сертифіката, або будь-яких інших засобів;

б) перевіряє коректність маркера $TokenAB$ шляхом:

– перевірки цифрового підпису, що міститься в маркері;

– перевірки відповідності випадкового числа R_B, що було надіслане об'єкту A на кроці (1), та випадкового числа, що міститься в підписаних даних маркера $TokenAB$;

– (за наявності) порівняння ідентичності значення поля ідентифікатора B у підписаних даних маркера $TokenAB$ та розпізнавального ідентифікатора об'єкта B.

4. Об'єкт B генерує та надсилає маркер $TokenBA$ об'єкту A, а також (необов'язково) свій сертифікат.

5. після отримання повідомлення, що містить $TokenBA$, об'єкт A виконує кроки, аналогічні крокам об'єкта B на третьому кроці:

а) впевнюється в тому, що володіє дійсним відкритим ключем об'єкта B, за допомогою або сертифіката, або будь-яких інших засобів;

б) перевіряє коректність маркера $TokenBA$ шляхом:

– перевірки цифрового підпису, що міститься в маркері;

– перевірки відповідності випадкового числа R_A, що було надіслане об'єкту B на кроці (2) та випадкового числа, що міститься в підписаних даних маркера $TokenBA$;

– (за наявності) порівняння ідентичності значення поля ідентифікатора A в підписаних даних маркера $TokenBA$ та розпізнавального ідентифікатора об'єкта A.

А також додатково до цих кроків перевіряє відповідність випадкового числа R_B, що міститься в підписаних даних маркера $TokenBA$, та випадкового числа, отриманого на кроці (1).

Ініціатором механізму встановлення взаємної автентифікації є об'єкт B. Цей механізм використовує запит на перевірку пароля R_B об'єкта B, запит на перевірку пароля R_A об'єкта A, загальні характеристики обраних перевірників B для другого проходу, та A для третього проходу, заявлену ІА як $Text2$ для об'єкта A і $Text4$ для об'єкта B, яка схована від порушника. За класифікацією вразливостей механізмів автентифікації, поданих у стандарті ISO/IEC 10181-2 цей механізм підпадає під клас 4 «Механізми, що захищені від розкриття заявленої ІА та атак типу «Повтор» на одного та різних «перевірників», проміжний клас 4*b* «механізми із запитом паролю».

Стійкість даного механізму взаємної автентифікації ґрунтується на стійкості механізму двопрохідної однобічної автентифікації, що описано в ДСТУ ISO/IEC 9798-3, тому додатково необхідно визначити таке. Включення випадкового числа R_A в підписані дані маркера $TokenAB$ спрямовано на запобігання атаці, у ході якої об'єкт B може до початку механізму автентифікації отримати цифровий підпис об'єкта A, на даних, що обрано об'єктом B. Цей засіб захисту може знадобитися у випадку, коли об'єкт A використовує свій ключ автентифікації не тільки для здійснення автентифікації об'єктів. Включення випадкового числа R_B у маркер $TokenBA$, якщо це буде необхідно з міркувань безпеки, які вимагають порівняння об'єктом A випадкового числа R_B з маркеру $TokenBA$ та значення R_B, одержаного із запиту на автентифікацію, не забезпечує захист об'єкта B. Це є наслідком того, що значення R_B відомо об'єкту A ще перед вибором випадкового числа R_A. Таким чином, для надання додаткового захисту об'єкт B може вставити додаткове випадкове число R'_B в текстове поле $Text5$ та в підписані дані маркера $TokenBA$.

Наведений механізм автентифікації можна використовувати разом із протоколами встановлення та розподілення ключів, що наведено в стандарті ДСТУ ISO/IEC 11770-2, 3 та ДСТУ ISO/IEC 15946-3, із застосуванням для управління ключовою інформацією. Наприклад, для встановлення секретного ключа з підтвердженням і взаємної автентифікації, де ініціатором є об'єкт B, можна цей механізм подати таким чином.

Об'єкт B одержує маркер $TokenAB$, перевіряє його та формує за допомогою криптографічної контрольної функції v та ключа K_{AB} секретний ключ

$$K=v_{K_{AB}}(R_A||R_B),$$

та зашифровує на цьому ключі маркер $TokenBA$

$$TokenBA = e_K(R_B \,||\, R_A \,||\, A \,||\, Text5 \,||\, sS_B(R_B \,||\, R_A \,||\, A \,||\, Text4)). \quad (6.18)$$

Об'єкт A одержує з маркера, що сформовано на першому проході необхідні дані, виробляє ключ K та розшифровує одержаний маркер $TokenBA$. А далі робить усі перевірки згідно з вимогами перевірки даного механізму, як описано вище.

Таким чином, модифікований механізм може застосовуватись для взаємної автентифікації користувача, що використовує електронний ключ, з РС та встановлення секретного ключа з підтвердженням для криптографічного тунелю між електронним ключем користувача та модулем захисту РС, цей же ключ може або повинен використовуватись як ключ криптографічного тунелю.

6.10.2. Криптографічні протоколи автентифікації користувачів і робочих станцій згідно з ДСТУ ISO/IEC 15946-3

Проведений аналіз та дослідження дозволили вибрати як альтернативи протоколу автентифікації РС та користувача, що наведений в 6.10.1, протокол узгодження ключів типу Діффі-Геллмана з двома цифровими підписами та підтвердженням ключів (KADH2SKC) [37, 36].

Цей механізм узгодження ключів установлює розділену таємницю та/або ключ між суб'єктами A і B за три обміни повідомленнями. Він здійснюється за допомогою електронного ключа. Участь користувача полягає в тому, що він встановлює в РС (сервер) електронний ключ і вводить пароль доступу до електронного ключа. Далі автоматично здійснюється взаємна автентифікація електронного ключа та РС (модуля захисту РС).

6.10.2.1. Сутність і характеристики протоколу

Протокол узгодження ключів типу Діффі-Геллмана з двома цифровими підписами та підтвердженням ключів (KADH2SKC) [37, 36] полягають в такому.

Налаштування

Перед процесом узгодження розділеної таємниці додатково до спільної інформації необхідно:

1) для кожного суб'єкта встановити особистий ключ цифрового підпису та відкритий ключ перевірки, відповідно до взаємноузгодженої схеми цифрового підпису;

2) для кожного суб'єкта забезпечити доступ до автентичної копії відкритого ключа перевірки іншої сторони;

3) установити всі параметри, що мають використовуватись у перетвореннях цифрового підпису;

4) установити функцію f обчислення криптографічного контрольного значення.

Механізм узгодження ключів

Нехай особисте та відкрите перетворення цифрового підпису суб'єкта X позначають S_x та V_x відповідно; пара (S_x, V_x) може позначати будь-яку систему цифрового підпису, наприклад, одну з тих, що визначено у стандартах ДСТУ 4145-2002, ISO/IEC 9796, ISO/IEC 14888 або ISO/IEC 15946-2.

Формування маркера ключа (*A*)

Суб'єкт А випадково генерує таємне значення r_A, що належить діапазону $[1, n-1]$, обчислює $r_A G$, формує маркер ключа

$$KT_{A1} = r_A G \tag{6.19}$$

та надсилає його суб'єкту *B*.

Формування маркера ключа (*B*)

Суб'єкт *B* повинен перевірити, що маркер KT_{A1} дійсно є точкою еліптичної кривої (див. ДСТУ ISO/IEC 15946-1, де описана процедура перевіряння). Суб'єкт *B* випадково генерує таємне значення r_B, що належить діапазону $\{1,\ldots,n-1\}$, обчислює $r_B G$ та обчислює розділену таємницю

$$K_{AB} = (r_B \cdot l)\,(h \cdot KT_{A1}), \tag{6.20}$$

формує підписаний маркер ключа

$$KT_{B1} = S_B(DB_1) \,\|\, f_{K_{AB}}(DB_1), \tag{6.21}$$

де

$$DB_1 = r_B G \,\|\, KT_{A1} \,\|\, A\ [\|Text1] \tag{6.22}$$

та надсилає його суб'єкту *A*.

Примітка. Для зменшення кількості переданих даних у разі використання схем цифрового підпису з додатком, надлишкове значення KT_{A1} можна не повертати разом з блоком KT_{B1}, але його необхідно включати в процес обчислення цифрового підпису.

Обробка маркера ключа (A)

Суб'єкт *A* перевіряє цифровий підпис маркера ключа KT_{B1} суб'єкта *B*, використовуючи відкритий ключ перевіряння суб'єкта *B*. Якщо використовують схему цифрового підпису з відновленням повідомлення, тоді ця обробка охоплює відновлення блоку даних DB_1 з підпису і перевіряння того, що розпізнавальний ідентифікатор суб'єкта *A* та значення $r_A G$ містяться в цьому блоці. Якщо використовується схема цифрового підпису з додатком, тоді ця обробка охоплює відтворення блоку даних DB_1, використовуючи значення KT_{A1} розпізнавального ідентифікатора суб'єкта *A* та одержаного значення $r_B G$, а також перевіряння цифрового підпису цього блоку даних.

Суб'єкт *A* повинен перевірити, що значення $r_B G$, одержане з KT_{B1}, дійсно є точкою еліптичної кривої (див. ДСТУ ISO/IEC 15946-1, де описана процедура перевіряння). Якщо перевіряння пройшло успішно, то суб'єкт *A* обчислює спільний ключ

$$K_{AB} = (r_A \cdot l)\,(h \cdot r_B G). \tag{6.23}$$

Використовуючи K_{AB}, суб'єкт *A* перевіряє криптографічне контрольне значення $f_{K_{AB}}(DB_1)$. Далі суб'єкт *A* формує підписаний маркер ключа

$$KT_{A2} = S_A(DB_2) \,\|\, f_{K_{AB}}(DB_2), \tag{6.24}$$

де

$$DB_2 = r_A G \,\|\, r_B G \,\|\, B\ [\|Text2], \tag{6.25}$$

та надсилає його суб'єкту *B*.

Примітка. Для зменшення кількості переданих даних при використанні схем цифрового підпису з додатком, можна не повертати значення $r_A G$ та $r_B G$ разом з блоком KT_{A2}, але їх необхідно включати в процес обчислення цифрового підпису.

Обробка маркера ключа (*B*)

Суб'єкт B перевіряє цифровий підпис маркера ключа KT_{A2} суб'єкта A, використовуючи відкритий ключ перевіряння суб'єкта A. Якщо треба використовувати схему цифрового підпису з відновленням повідомлення, то ця обробка охоплює відновлення блоку даних DB_2 з підпису та перевіряння, що розпізнавальний ідентифікатор суб'єкта B та значення $r_A G$ і $r_B G$ містяться в цьому блоці. Якщо треба використовувати схему цифрового підпису з додатком, то ця обробка охоплює перетворення блоку даних DB_2, використовуючи значення KT_{A1}, KT_{B1} і розпізнавального ідентифікатора суб'єкта B та перевіряння цифрового підпису цього блоку даних.

Якщо перевіряння пройшли успішно, суб'єкт B перевіряє криптографічне контрольне значення $f_{K_{AB}}(DB_2)$, використовуючи спільний ключ

$$K_{AB} = (r_B \cdot l)\,(h \cdot KT_{A1}). \tag{6.26}$$

6.10.2.2. Функція вироблення ключа зі спільної таємниці

Відзначимо, що використання розділюваної таємниці, виробленої відповідно до наведеного протоколу як ключа для симетричних криптографічних систем, без подальшої обробки не рекомендується. Найчастішим буде випадок, коли форма розділюваної таємниці не буде відповідати вимогам до форми розділюваного симетричного ключа, тому необхідна деяка подальша обробка. Таємниця, що розділюється, може мати арифметичні властивості та взаємозалежності, які в результаті не дають можливості обирати розділюваний таємний ключ з повного простору потенційно можливих ключів. Тому бажано розділювану таємницю перетворювати за допомогою функції вироблення ключа, наприклад, за рахунок використання геш-функції. Необхідно враховувати, що використання функції вироблення ключа, що не відповідає вимогам, у схемі узгодження ключів компрометує безпеку цієї схеми.

Це пов'язано з тим, що таємниця, яка розділюється, не завжди відповідає вимогам, що висуваються до симетричних ключів. Наприклад, така таємниця може не задовольняти вимогам рівноймовірності та незалежності вибору із повної множини можливих ключів. Зазначений недолік може бути виключений унаслідок додаткового перетворення розділюваної таємниці. Для перетворення рекомендується використовувати функцію ДСТУ ISO/IEC 15946-3, тобто у разі використання розділюваної таємниці без перетворення протоколи узгодження ключів можуть бути послаблені. Крім того, у більшості випадків довжина розділюваної таємниці не співпадає з довжиною розділюваного таємного ключа. Зазвичай таємниця, що розділюється, має довжину більшу, ніж довжина розділюваного таємного ключа.

Функція вироблення ключа має виробляти ключі, які є обчислено нерозрізненими від ключів, які генерують випадково. Також функція вироблення ключа на основі таких вхідних даних, як таємниця, що розділюється, та набір параме-

трів вироблення ключа, має виробляти вихідні дані необхідної довжини. Також функція вироблення ключів перед узгодженням таємного ключа у механізмі встановлення ключа має бути узгодженою належним чином для обох взаємодіючих сторін. У [36, 37] наведено три приклади функцій вироблення ключів.

6.10.2.3.Особливості використання та властивості кофакторного множення

Механізм узгодження ключів, що наведений у п. 6.10.2.1, вимагає, щоб особистий ключ користувача або маркер ключа був зв'язаний з відкритим ключем або маркером ключа іншого об'єкта. Якщо при цьому відкритий ключ або маркер ключа іншого об'єкта є неправильним (наприклад, він не є точкою еліптичної кривої, або не входить у підгрупу порядку n), то виконання цієї операції може призводити до того, що деякі біти особистого ключа стануть відомими порушнику. Прикладом такої атаки є «атака в малу підгрупу». Ще до більших вразливостей може призвести той факт, що викривленою є базова точка.

Одним із методів запобігання «атаки в малу підгрупу» або аналогічних атак є перевірка відкритих ключів і маркерів ключів, а також базової точки, отриманих від іншої сторони, використовуючи механізм перевірки відкритого ключа. У стандарті ISO/IEC 15946-1 [30–32] наведено механізм перевірки відкритого ключа.

Як альтернативу для перевірки порядку відкритого ключа або маркера ключа може бути використано метод кофакторного множення. Для здійснення кофакторного множення [30–32] використовують значення h та l, які визначено нижче.

Існують такі варіанти виконання кофакторного множення:

Якщо використовують кофакторне множення й потрібна несумісність з об'єктами, які не використовують кофакторне множення, то $h = \#E/n$ та $l = 1$. Якщо обирають цей варіант, обидві залучені сторони повинні узгодити використання цього варіанту, інакше механізм не буде діяти.

Якщо використовують кофакторне множення й потрібна сумісність з об'єктами, які не використовують кофакторне множення, то $h = \#E/n$ та $l = h^{-1} \bmod n$. Якщо обирають цей варіант, тоді механізми, які наведено в 6.10.2.1, є сумісними з ISO/IEC 11770-3.

Примітка. Значення $h^{-1} \bmod n$ завжди буде існувати, оскільки необхідно, щоб значення n було більше, ніж $\sqrt[4]{q}$ [див. ISO/IEC 15946-1] та відповідно $\gcd(n, h) = 1$.

Якщо немає необхідності використовувати кофакторне множення, тоді існує один варіант. Якщо не використовують кофакторне множення, то $h = 1$ та $l = 1$. Якщо обрано цей варіант, тоді механізм є сумісним з ISO/IEC 11770-3 [36–37].

Також, незалежно від того, чи використовують кофакторне множення, та від того, чи обрано тип сумісності, якщо розділюваний ключ (або складовий елемент розділюваного ключа) приймає значення точки нескінченності (0_E), то користувач повинен прийняти рішення, що узгодження ключів пройшло невдало.

Необхідно зазначити, що найбільш доречним є застосування операцій перевірки відкритого ключа або кофакторного множення, якщо не виконується автентифікація відкритого ключа або маркера ключа іншого об'єкта, або відкритий ключ користувача є довгостроковим. Виконання перевіряння відкритого ключа та кофакторного множення, що застосовуються для довгострокових ключів та короткострокових ключів відповідно, можуть мати певні переваги.

6.10.2.4. Аналіз властивостей протоколу встановлення ключів типу Діффі-Геллмана з двома електронними цифровими підписами та підтвердженням ключів

Проведемо аналіз криптографічного протоколу, що наведений у п. 6.10.2.1. Попередні дослідження дозволили визначити, що при його застосуванні забезпечуються такі властивості:

а) взаємна автентифікація об'єктів (суб'єктів);

б) взаємна криптоживучість встановлених ключів;

в) підтвердження встановленого ключа;

г) взаємна неявна автентифікація ключа;

д) кількість обмінів повідомленнями при автентифікації – 3.

Окрім того, для реалізації протоколу необхідно узгодити та використовувати функцію обчислення криптографічних контрольних значень

$$f_{K_{AB}}(DB_1) \cdot f_{K_{AB}}(DB_2)$$

Таким чином, протокол узгодження ключів типу Діффі-Геллмана з двома цифровими підписами та підтвердженням ключів (KADH2SKC) призначений для встановлення спільної таємниці (ключів) між суб'єктами *A* та *B* та забезпечує це встановлення за три проходи. Перед виконанням протоколу необхідно узгодити функцію обчислення криптографічного контрольного значення та функцію вироблення й перевірки електронного цифрового підпису. Для обчислення криптографічних контрольних значень повинно бути використане симетричне криптоперетворення типу «код автентифікації повідомлення» (використання імітовставки) згідно з ГОСТ 28147-89 або іншого блокового симетричного шифру. Детально питання вибору та здійснення обчислень криптографічних контрольних значень розглянуто в ISO/IEC 9797-1, ISO/IEC 9797-2, ISO/IEC 9798-3:2002 [213]. Як ЕЦП може бути використаний національний стандарт ДСТУ 4145-2002 [35].

Як важливі також відзначимо такі властивості й характеристики:

1) *обсяг попередньо одержаної інформації*. Аналіз показує, що для виконання протоколу необхідно попередньо встановити загальні параметри та для узгодженого алгоритму виробити особисті ключі. Також повинно бути забезпечено доступ до сертифікатів усіх суб'єктів, з якими здійснюється взаємодія, встановлено всі параметри криптографічних перетворень ЕЦП, а також встановлено функцію обчислення криптографічного контрольного значення;

2) *кількість проходів*. Алгоритм вимагає при встановленні спільної таємниці (ключа) виконання трьох проходів. Порушник (криптоаналітик) може визначити факт встановлення спільної таємниці (ключа) та перехопити всі відкриті ключі ініціатора й відповідача протоколу;

3) *кількість ключів (ключових пар)*. Для виконання протоколу необхідно, щоб суб'єкт-ініціатор мав одну пару особистий/ відкритий ключ, суб'єкт-відповідач також мав одну пару особистий/ відкритий ключ. Усі пари ключів мають бути генеровані під час виконання протоколу. Загальна кількість ключових пар, що використовуються під час виконання алгоритму, дорівнює двом. Окрім того, вважається, що суб'єкти мають сертифіковані пари ключів для алгоритмів цифрового підпису. Причому відкриті ключі перевірки цифрового підпису повинні бути доступними об'єктам;

4) *додаткова інформація.* Протокол не потребує встановлення додаткової інформації, як таємної, так і відкритої;

5) *пасивна атака.* Під час цієї атаки криптоаналітик намагається перехопити всі повідомлення, що передаються при узгодженні ключів. При використанні інтерактивного протоколу встановлення ключів типу Діффі-Геллмана між сторонами відбуваються три раунди передачі даних – суб'єкт-ініціатор та суб'єкт-відповідач передають один одному свої відкриті ключі. При цьому криптоаналітик теоретично може перехопити всі повідомлення, тобто перехопити обидві пари відкритих ключів. Для розкриття будь-якої інформації (значення спільної таємниці, значення особистих ключів сеансу) порушник має встановити за відомими відкритими ключами та базовою точкою особистий ключ, тобто вирішити завдання розв'язання дискретного логарифмічного рівняння в групі точок еліптичної кривої [7, 9, 10, 30–32]. Але визначення особистих ключів сеансових пар суб'єктів не призведе до реалізації атаки типу «Повне розкриття», оскільки визначений порушником особистий ключ більше не буде використовуватись у системі, і на основі отриманого ключа можна встановити тільки ключ сеансу, який уже використано, і виконати розкриття тільки тієї інформації, що захищена з використанням цього ключа;

6) *активна атака.* Ця атака вимагає взаємодії між суб'єктами під час встановлення ключів. У протоколі застосовується три раунди взаємодії між учасниками протоколу – передача відкритого сеансового ключа суб'єкта-ініціатора суб'єкту-відповідачу та навпаки, а також передача маркера контролю цілісності й справжності суб'єкта-ініціатора. Для виконання атаки порушник може використовувати три стратегії. Вибір сценарію залежить від мети, яку переслідує порушник. Можливі такі варіанти:

а) завадити суб'єктам, які взаємодіють, та виробити ключ. У такому випадку порушник може перехоплювати та модифіковувати повідомлення. За таких умов суб'єкти не зможуть виробити однакову спільну таємницю.

б) сформувати спільну таємницю з одним із суб'єктів. Здійснення такої атаки можливе тільки на початковому етапі роботи протоколу. Тобто порушник може сформувати пару ключів сеансу та надіслати її відповідачеві, а також отримати від відповідача його відкритий ключ, перевірити його цілісність і справжність та сформувати спільний ключ. Але протокол не буде завершено вдало, бо під час відповіді порушник не зможе правильно підписати повідомлення (хоча й зможе правильно обчислити криптографічну контрольну суму). Для забезпечення захисту від цієї атаки (навіть якщо вона не може завершитись вдало) необхідно вжити заходів щодо забезпечення цілісності й справжності відкритого ключа суб'єкта-ініціатора під час першої передачі, тобто підписати перший ключ сеансу суб'єкта-ініціатора.

в) атака типу «Об'єкт посередині» неможлива в такому протоколі, бо два повідомлення з трьох підписуються, тому їх підміна чи спроба порушника сформувати спільні ключі з обома суб'єктами неможлива.

г) загальний рівень безпеки щодо визначення спільного ключа. Безпека спільного ключа повністю базується на проблемі дискретного логарифму в групі точок еліптичної кривої. Інші спроби порушника з'ясувати таємний ключ одного з абонентів чи спільну таємницю не призведуть до розкриття спільного ключа, бо в такому випадку суб'єкт-відповідач відмовиться від співпраці з порушником, оскільки той не зможе правильно підписати останнє повідомлення.

Рекомендації та пропозиції

Протокол узгодження ключів типу Діффі-Геллмана з двома цифровими підписами та підтвердженням ключів (KADH2SKC)) ДСТУ ISO/IEC 15946-3 забезпечує взаємну явну автентифікацію суб'єктів A та B, а також взаємну криптоживучість ключів суб'єктів A та B. Цей протокол необхідно застосовувати на практиці, оскільки він найповніше забезпечує безпечне встановлення ключів та спільної таємниці.

6.10.3. Криптографічні протоколи автентифікації користувачів і робочих станцій згідно ДСТУ ISO/IEC 11770-3

6.10.3.1. Сутність і характеристики протоколу

Проведений аналіз і дослідження дозволили вибрати як один із перспективних протоколів автентифікації РС та користувача «Протокол узгодження ключів 3» із цифровим підписом та підтвердженням ключа» [21, 22].

Протокол 3 ДСТУ ISO/IEC 11770-3 задається формально, тобто, по суті, він представлений у стандарті у вигляді механізму (рис. 6.23). При його використанні необхідно вибрати криптографічний алгоритм ЕЦП. З урахуванням національних вимог будемо орієнтуватись на національний стандарт ДСТУ 4145-2002, хоча це не принципово.

Аналіз показує, що цей механізм узгодження ключів установлює розділену таємницю та/або ключ між суб'єктами A і B за один обмін повідомленням. Він здійснюється за допомогою електронного ключа. Участь користувача полягає в тому, що він встановлює в РС (сервер) електронний ключ і вводить пароль доступу до електронного ключа. Далі автоматично здійснюється взаємна автентифікація електронного ключа та РС (модуля захисту РС). Для автентифікації A та B, а також B та A необхідно здійснювати незалежно автентифікацію.

Протокол 3 згідно ДСТУ ISO/IEC 11770-3 забезпечує встановлення розділюваного таємного ключа між суб'єктами A і B за один прохід із взаємною неявною автентифікацією ключа й автентифікацією суб'єктом B суб'єкта A.

Повинні виконуватись такі вимоги:

1) суб'єкт A має асиметричну систему підпису (S_A, V_A);

2) суб'єкт B має доступ до автентифікованої копії відкритого перетворення перевіряння V_A;

3) суб'єкт B має систему узгодження ключів з ключами (h_B, p_B);

4) суб'єкт A має доступ до автентифікованої копії відкритого ключа p_B для узгодження ключів суб'єкта B;

5) *TVP*: як *TVP* повинна використовуватись або позначка часу, або порядковий номер. Якщо використовується позначка часу, необхідні надійні та синхронізовані таймери; якщо використовується порядковий номер, то необхідна можливість підтримання та контролювання двосторонніх лічильників;

6) суб'єкти A і B мають узгоджену криптографічну контрольну функцію f (аналогічну стандартизованій у проекті ДСТУ ISO/IEC 9797) і шлях включення розділюваного таємного ключа K_{AB} як ключа цієї криптографічної контрольної функції.

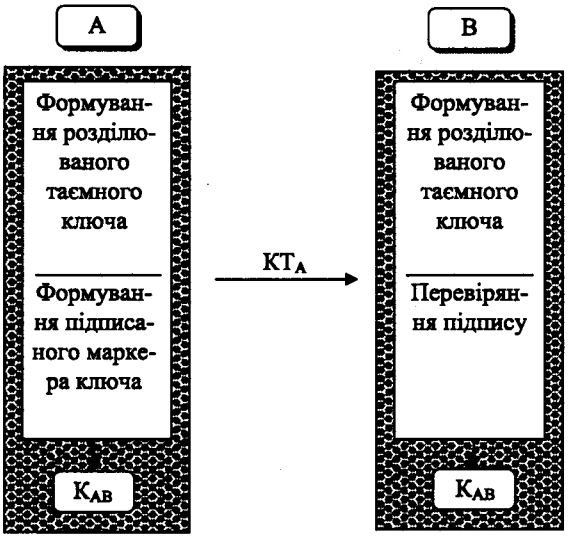

Рис. 6.23. Узгодження ключів, протокол 3

Формування розділюваного таємного ключа

Суб'єкт A генерує випадкове таємне число $r \in H$, обчислює $F(r,g)$ та обчислює розділюваний таємний ключ:

$$K_{AB} = F(r, p_B). \tag{6.27}$$

Суб'єкт A, використовуючи розділюваний таємний ключ K_{AB}, обчислює криптографічне контрольне значення $f_{K_{AB}}(A \parallel TVP)$ шляхом об'єднання свого розрізнювального ідентифікатора і порядкового номера або позначки часу TVP.

Формування підписаного маркера ключа

Суб'єкт A підписує криптографічне контрольне значення $f_{K_{AB}}(A \parallel TVP)$ з використанням свого особистого перетворення підписування S_A. Потім суб'єкт A формує маркер ключа, який складається з його розрізнювального ідентифікатора, вхідного значення $F(r, g)$, TVP, підписаного криптографічного контрольного значення і деяких необов'язкових даних ($Text1$):

$$KT_{A1} = A \parallel F(r,g) \parallel TVP \parallel S_A(f_{K_{AB}}(A \parallel TVP)) \parallel Text1 \tag{6.28}$$

і надсилає його суб'єкту B.

Формування розділюваного таємного ключа

Суб'єкт B виділяє $F(r, g)$ з одержаного підписаного маркера ключа і обчислює розділюваний таємний ключ, використовуючи свій особистий ключ h_B для узгодження ключів:

$$K_{AB} = F(h_B, F(r, g)). \tag{6.29}$$

Суб'єкт B, використовуючи розділюваний таємний ключ K_{AB}, обчислює криптографічне контрольне значення від розрізнювального ідентифікатора суб'єкта A і TVP.

Перевіряння підпису

Суб'єкт B перевіряє підпис суб'єкта A, використовуючи відкрите перетворення перевіряння V_A, а з тим цілісність і справжність одержаного маркера KT_{A1}. Потім суб'єкт B підтверджує, що маркер не є повтором у часі, та засвідчує його своєчасність, аналізуючи TVP.

Протокол 3 має такі властивості:

1) Особистий ключ є ключем сеансу, тобто він завжди буде новим. Але ініціатором вироблення ключа може бути тільки суб'єкт A.

2) Кожен із суб'єктів впливає на вироблення розділюваного таємного ключа, оскільки кожен із них при його виробленні використовує свій особистий ключ: суб'єкт A – ключ сеансу r, суб'єкт B – статичний ключ h_B, а також відкриті ключі P_B та $F(r, g)$ суб'єктів B та A відповідно.

3) Протокол є однопрохідним, тобто він вимагає передавання відкритого маркера ключа від суб'єкта A суб'єкту B. Суб'єкт A повинен здійснити два асиметричних криптографічних перетворення при обчисленні K_{AB} та при виробленні електронного цифрового підпису. Суб'єкт B також повинен виконати два асиметричних перетворення – при перевірці електронного цифрового підпису та обчисленні розділюваного таємного ключа. Як суб'єкт A, так і суб'єкт B попередні обчислення здійснити не можуть, оскільки розділюваний таємний ключ є ключем сеансу.

4) Основною вимогою до третьої сторони є виготовлення або використання сертифікату відкритого ключа P_B та підтримування його життєвого циклу, наприклад, обслуговування.

5) Як відкритий ключ повинен використовуватись сертифікат відкритого ключа P_B. Можливі різні способи його виготовлення та обслуговування.

6) У протоколі забезпечується неспростовність суб'єкта A, що досягається застосуванням електронного цифрового підпису S_A. Хоча суб'єкт B й застосовує особистий ключ h_B, але при цьому неспростовність B не забезпечується, оскільки розділюваний таємний ключ K_{AB} може обчислити також суб'єкт A.

7) Забезпечується криптографічна живучість сеансового ключа h, оскільки він використовується тільки один раз.

8) На протокол можливо здійснення пасивних атак типу «Повне розкриття». Причому повне розкриття особистого сеансового ключа h призводить до компрометації тільки одного розділюваного таємного ключа.

6.10.3.2. Функція вироблення ключа зі спільної таємниці

Обчислення значення криптографічної контрольної суми може здійснюватись з використанням стандарту (проекту) ДСТУ ISO/IEC 9797. Використання розділюваної таємниці, що вироблена відповідно до наведеного протоколу, як ключа для симетричних криптографічних систем без подальшої обробки не рекомендується. Найчастішим буде випадок, коли форма розділюваної таємниці не буде відповідати вимогам до форми розділюваного симетричного ключа, тому необхідна деяка додаткова обробка. При цьому розділювана таємниця має арифметичні властивості та взаємозалежності, які в результаті не дають можливості обирати розділюваний таємний ключ з повного простору потенційно можливих ключів. Тому бажано розділювану таємницю перетворювати за допомогою функції вироблення ключа, наприклад, використання геш-функції. Використання

функції вироблення ключа, що не відповідає вимогам у схемі узгодження ключів, компрометує безпеку цієї схеми.

Зазначене пов'язане з тим, що розділювана таємниця не завжди відповідає вимогам, які висуваються до симетричних ключів. Наприклад, така таємниця може не задовольняти вимогам рівноймовірності та незалежності вибору із повної множини можливих ключів. Зазначений недолік може бути виключений засобом додаткового перетворення розділюваної таємниці. Для перетворення рекомендується використовувати функцію вироблення ключа, у якій використовується, наприклад, геш-функція. В іншому випадку, тобто у випадку використання розділюваної таємниці без перетворення, протоколи узгодження ключів можуть бути послаблені. Крім того, у більшості випадків довжина розділюваної таємниці не співпадає з довжиною розділюваного таємного ключа. Зазвичай, таємниця, що розділюється, має довжину більшу, ніж довжина розділюваного таємного ключа.

Функція вироблення ключа має виробляти ключі, які є обчислено нерозрізненими від ключів, що генерують випадково. Функція вироблення ключа на основі таких вхідних даних, як розділювана таємниця та набір параметрів вироблення ключа, має виробляти вихідні дані необхідної довжини. Причому функція вироблення ключів узгодженням таємного ключа в механізмі встановлення ключа має бути узгодженою належним чином для двох сторін.

Якщо використовується кофакторне множення, то необхідно механізм реалізовувати згідно з п. 6.10.2.3 цього розділу.

6.10.4. Порівняння та вибір криптографічних протоколів автентифікації РС і користувачів з електроним ключем та встановлення ключів

6.10.4.1. Оцінка механізму та криптографічного протоколу автентифікації РС і користувачів з електронним ключем та встановлення ключів на основі використання ДСТУ ISO/IEC 9798-3

1. Детальний аналіз показав, що в групі асиметричних перетворень, поданих у стандарті ДСТУ ISO/IEC 9798-3, для доказу ідентифікаційних даних пред'явника, що передаються перевірнику, використовуються алгоритми асиметричних цифрових підписів. Пред'явник формує цифровий підпис, використовуючи свій особистий ключ від заявлених даних, розпізнавальний ідентифікатор, унікальні числа й унікальні характеристики перевірника. Перевірник одержує цифровий підпис разом із деякими даними, одержує сертифікат відкритого ключа або від пред'явника, або від уповноваженого на розподіл сертифікатів і перевіряє цифровий підпис, використовуючи як вхідні дані перевірочну інформацію, розпізнавальний ідентифікатор та інші дані, необхідні для перевірки цифрового підпису.

2. Щодо об'єктів автентифікації та механізмів автентифікації в стандарті ISO/IEC 9798-3 висуваються такі вимоги. Під час проходження автентифікації об'єкт підтверджує свою ідентичність шляхом пред'явлення доказу того, що він володіє знанням свого особистого ключа цифрового підпису. Для цього за допомогою особистого ключа виробляється електронний цифровий підпис від певних даних. Цифровий підпис може бути перевірений будь-яким об'єктом, який має доступ до відкритого ключа (сертифіката) електронного цифрового підпису.

3. Ініціатором механізму встановлення взаємної автентифікації є об'єкт B. Цей механізм використовує запит на перевірку пароля R_B об'єкта B, запит на перевірку пароля R_A об'єкта A, загальні характеристики обраних перевірників B для другого проходу та A для третього проходу, заявлену ІА як $Text2$ для об'єкта A та $Text4$ для об'єкта B, яка захищена від порушника.

4. За класифікацією вразливостей механізмів автентифікації, що подані в стандарті ISO/IEC 10181-2 та наведені в п. 6.5, цей механізм підпадає під клас 4 «Механізми, що захищені від розкриття заявленої ІА та атак типу «Повтор» на одного та різних перевірників», проміжний клас 4*b* «Механізми із запитом пароля».

Стійкість цього механізму взаємної автентифікації ґрунтується на стійкості механізму двопрохідної однобічної автентифікації, що описано в ДСТУ ISO/IEC 9798-3, тому додатково необхідно визначити таке. Включення випадкового числа R_A в підписані дані маркера $TokenAB$ спрямовано на запобігання атаці, у ході якої об'єкт B може до початку механізму автентифікації отримати цифровий підпис об'єкта A на даних, що обрано об'єктом B. Цей засіб захисту може знадобитись у випадку, коли об'єкт A використовує свій ключ автентифікації не тільки для здійснення автентифікації об'єктів. Включення випадкового числа R_B у маркер $TokenBA$, якщо це необхідно з міркувань безпеки, які вимагають порівняння об'єктом A випадкового числа R_B з маркеру $TokenBA$ та значення R_B, одержаного із запиту на автентифікацію, не забезпечує захист об'єкта B. Це є наслідком того, що значення R_B відомо об'єкту A ще перед вибором випадкового числа R_A. Для надання додаткового захисту об'єкт B може вставити додаткове випадкове число R'_B в текстове поле $Text5$ та в підписані дані маркера $TokenBA$.

5. Механізм (6.10.2.1) можна використовувати разом з протоколами встановлення та розподілення ключів, що наведено в стандарті ДСТУ ISO/IEC 11770-2, 3 та ДСТУ ISO/IEC 15946-3 для управління ключовою інформацією.

6. Таким чином, модифікований механізм може застосовуватись для взаємної автентифікації користувача, що використовує електронний ключ, з РС та встановлення секретного ключа з підтвердженням для криптотунелю між електронним ключем користувача та модулем захисту РС. Цей ключ також може або повинен використовуватись як ключ криптотунелю.

6.10.4.2. Оцінка механізму та криптографічного протоколу автентифікації РС і користувачів з електронним ключем та встановлення ключів на основі використання ДСТУ ISO/IEC 15946-3

1. Протокол узгодження ключів типу Діффі-Геллмана з двома цифровими підписами та підтвердженням ключів (KADH2SKC) [36, 37] установлює розділену таємницю та/або ключ між суб'єктами A і B за три обміни повідомленнями. Він здійснюється за допомогою електронного ключа. Участь користувача полягає в тому, що він встановлює в РС (сервер) електронний ключ і вводить пароль доступу до електронного ключа. Далі автоматично здійснюється взаємна автентифікація електронного ключа та РС (модуля захисту РС).

2. Протокол, що наведений у 6.10.2.1, має такі властивості:

а) забезпечує взаємну автентифікацію об'єктів (суб'єктів);

б) забезпечує взаємну криптоживучість встановлених ключів;

в) забезпечує підтвердження встановленого ключа;

г) забезпечує взаємну неявну автентифікацію ключа;

д) кількість обмінів повідомленнями – 3.

Крім того, для реалізації протоколу необхідно узгодити та використовувати функцію обчислення криптографічних контрольних значень

$$f_{K_{AB}}(DB_1) \cdot f_{K_{AB}}(DB_2).$$

Протокол (6.10.2.1), призначений для встановлення спільної таємниці (ключів) між суб'єктами A та B, забезпечує це встановлення за три проходи. Перед виконанням протоколу необхідно узгодити функцію обчислення криптографічного контрольного значення та функцію вироблення й перевірки електронного цифрового підпису. Для обчислення криптографічних контрольних значень має бути використано симетричне криптоперетворення типу «код автентифікації повідомлення» (імітовставка) згідно з ГОСТ 28147-89 або іншим блоковим симетричним шифром, що дозволений для застосування. Як ЕЦП може бути використаний національний стандарт ДСТУ 4145-2002 [35].

3. *Обсяг попередньо одержаної інформації.* Аналіз показує, що для виконання протоколу попередньо необхідно встановити загальні параметри, для узгодженого алгоритму виробити особисті ключі. Також має бути забезпечений доступ до сертифікатів усіх суб'єктів, з якими здійснюється взаємодія, установлено всі параметри криптографічних перетворень ЕЦП, а також встановлено функцію обчислення криптографічного контрольного значення.

4. Алгоритм вимагає виконання трьох проходів при встановленні спільної таємниці (ключа). Криптоаналітик може визначити факт встановлення спільної таємниці (ключа) та перехопити всі відкриті ключі ініціатора й відповідача протоколу.

5. При використанні інтерактивного протоколу встановлення ключів типу Діффі-Геллмана між сторонами відбуваються три раунди передачі даних – суб'єкт-ініціатор і суб'єкт-відповідач передають один одному свої відкриті ключі. При цьому криптоаналітик теоретично може перехопити всі повідомлення, тобто перехопити обидві пари відкритих ключів. Для розкриття будь-якої інформації (значення спільної таємниці, значення особистих ключів сеансу) порушник має встановити за відомими відкритими ключами та базовою точкою особистий ключ, тобто вирішити завдання розв'язання дискретного логарифмічного рівняння в групі точок еліптичної кривої. Але визначення особистих ключів сеансових пар суб'єктів не призведе до реалізації атаки типу «Повне розкриття», оскільки визначений порушником особистий ключ більше не буде використовуватись у системі, і на основі отриманого ключа можна встановити тільки ключ сеансу, який уже відбувся, і виконати розкриття тільки тієї інформації, що захищена з використанням цього ключа.

6. Активна атака вимагає взаємодії між суб'єктами під час встановлення ключів. У протоколі три раунди взаємодії між учасниками протоколу – передача відкритого сеансового ключа суб'єкта-ініціатора суб'єкту-відповідачу та навпаки, а також передача маркера контролю цілісності й справжності суб'єкта-ініціатора. Для виконання атаки порушник може використовувати три сценарії. Вибір сценарію залежить від мети, яку переслідує порушник. Можливі такі варіанти.

1) Завадити суб'єктам, які взаємодіють, виробити ключ. У такому випадку порушник може перехоплювати й модифіковувати повідомлення. У цьому випадку суб'єкти не зможуть виробити однакову спільну таємницю.

2) Сформувати спільну таємницю з одним із суб'єктів. Здійснення такої атаки можливе тільки на початковому етапі роботи протоколу. Тобто порушник може сформувати пару ключів сеансу та надіслати її відповідачеві, а також отримати від відповідача його відкритий ключ, перевірити його цілісність і справжність і сформувати спільний ключ. Але протокол не буде завершено вдало, бо під час відповіді порушник не зможе правильно підписати повідомлення (хоча й зможе правильно обчислити криптографічну контрольну суму). Для забезпечення захисту від цієї атаки (навіть якщо вона не може завершитись вдало) необхідно прийняти заходи щодо забезпечення цілісності та справжності відкритого ключа суб'єкта-ініціатора під час першої передачі, тобто підписати перший ключ сеансу суб'єкта-ініціатора.

3) Атака типу «Об'єкт посередині» неможлива у такому протоколі, бо два повідомлення з трьох підписуються, тому їх підміна чи спроба порушника сформувати спільні ключі з обома суб'єктами неможлива.

7. *Загальний рівень безпеки щодо визначення спільного ключа.* Безпека спільного ключа повністю базується на проблемі дискретного логарифму в групі точок еліптичної кривої. Інші спроби порушника з'ясувати таємний ключ одного з абонентів чи спільну таємницю не призведуть до розкриття спільного ключа, бо в такому випадку суб'єкт-відповідач відмовиться від співпраці з порушником, оскільки той не зможе правильно підписати останнє повідомлення.

8. Протокол (6.4.2.1) ДСТУ ISO/IEC 15946-3 забезпечує взаємну явну автентифікацію суб'єктів A та B, а також взаємну криптоживучість ключів суб'єктів A та B. Цей протокол можна застосовувати на практиці, оскільки він найповніше забезпечує безпечне встановлення ключів і спільної таємниці.

6.10.4.3. Оцінка механізму та криптографічного протоколу автентифікації РС і користувачів з електронним ключем та встановлення ключів на основі використання ДСТУ ISO/IEC 11770-3

1. Проведений аналіз і дослідження показали, що протокол 6.10.3 автентифікації РС та користувача згідно ДСТУ ISO/IEC 11770-3 задається формально, тобто по суті він подний у стандарті у вигляді механізму. При його використанні необхідно вибрати криптографічний алгоритм ЕЦП, наприклад, національний стандарт ЕЦП ДСТУ 4145-2002 чи ISO/IEC 15946-2 та функції гешування ГОСТ 34.311-95 чи згідно ISO/IEC 10118-1, 2 (SHA-1, SHA-2 тощо).

2. Механізм узгодження ключів, що аналізується, встановлює розділену таємницю та/або ключ між суб'єктами A та B за один обмін повідомленням. Він здійснюється за допомогою електронного ключа. Участь користувача полягає в тому, що він встановлює в РС (сервер) електронний ключ і вводить пароль доступу до електронного ключа. Далі автоматично здійснюється взаємна автентифікація електронного ключа та РС (модуля захисту РС). Для автентифікації A та B, а також B та A необхідно здійснювати незалежну автентифікацію.

3. Протокол 3 згідно з ДСТУ ISO/IEC 11770-3 забезпечує встановлення розділюваного таємного ключа між суб'єктами A і B за один прохід із взаємною неявною автентифікацією ключа й автентифікацією суб'єктом B суб'єкта A.

4. Особистий ключ є ключем сеансу, тобто він завжди буде новим. Але ініціатором вироблення ключа може бути тільки суб'єкт A.

5. Кожен із суб'єктів впливає на вироблення розділюваного таємного ключа, оскільки кожен із них при його виробленні використовує свій особистий ключ: суб'єкт A – ключ сеансу r, суб'єкт B – статичний ключ h_B, а також відкриті ключі P_B та $F(r, g)$ суб'єктів B та A відповідно.

6. Протокол є однопрохідним, тобто він вимагає передавання відкритого маркера ключа від суб'єкта A суб'єкту B. Суб'єкт A повинен здійснити два асиметричних криптографічних перетворення при обчисленні K_{AB} та при виробленні електронного цифрового підпису. Суб'єкт B також повинен виконати два асиметричних перетворення – при перевірці електронного цифрового підпису та обчисленні розділюваного таємного ключа. Як суб'єкт A, так і суб'єкт B попередні обчислення здійснити не можуть, тому що розділюваний таємний ключ є ключем сеансу.

7. Основною вимогою до третьої сторони є виготовлення сертифікату відкритого ключа P_B та підтримування його життєвого циклу, наприклад обслуговування. Як відкритий ключ повинен використовуватись сертифікат відкритого ключа P_B. Можливі різні способи його виготовлення та обслуговування.

8. У протоколі забезпечується неспростовність суб'єкта A, що досягається застосуванням електронного цифрового підпису S_A. Хоча суб'єкт B й застосовує особистий ключ h_B, але при цьому неспростовність B не забезпечується, оскільки розділюваний таємний ключ K_{AB} може обчислити також суб'єкт A.

9. Забезпечується криптографічна живучість сеансового ключа r, оскільки він використовується тільки один раз.

10. На протокол можливе здійснення пасивних атак типу «Повне розкриття». Причому *повне розкриття особистого сеансового ключа* r призводить до компрометації тільки одного розділюваного таємного ключа.

6.10.5. Висновки та рекомендації щодо вибору криптографічного протоколу автентифікації РС і користувачів з електронним ключем та встановлення ключів

1. На основі аналізу та порівняння криптографічних механізмів і протоколів автентифікації, що подані в ДСТУ ISO/IEC 9798-3, ДСТУ ISO/IEC 15946-3 та ДСТУ ISO/IEC 11770-3, як основний механізм та на його основі криптографічний протокол автентифікації РС і користувачів з електронним ключем та встановлення ключів пропонується вибрати механізм 5.2.2 взаємної автентифікації із ISO/IEC 9798-3 [23, 24].

2. Криптографічний механізм і відповідний йому криптографічний протокол 5.2.2, за класифікацією вразливостей механізмів автентифікації згідно міжнародного стандарту ISO/IEC 10181-2, підпадає під найвищий 4-й клас захищеності «Механізми, що захищені від розкриття заявленої ІА та атак типу «Повтор» на одного та різних перевірників», проміжний клас 4*b* «Механізми із запитом паролю».

3. Згідно механізму 5.2.2 під час проходження автентифікації кожен об'єкт підтверджує свою ідентичність шляхом пред'явлення доказу того, що він володіє знанням свого особистого ключа (електронного) цифрового підпису. Цифровий

підпис може бути перевірений будь-яким об'єктом, який має доступ до відкритого ключа (сертифіката) електронного цифрового підпису.

4. Механізм 5.2.2 можна також використовувати разом із протоколами встановлення та розподілення ключів, що наведено у стандарті ДСТУ ISO/IEC 11770-2, 3 та ДСТУ ISO/IEC 15946-3 для управління ключовою інформацією.

5. З урахуванням національних вимог як стандарт електронного цифрового підпису в криптографічному протоколі автентифікації необхідно використовувати національний стандарт ДСТУ 4145-2002. За необхідності як електронний цифровий підпис можуть бути використані алгоритми, що представлені в ISO/IEC 15946-2.

6. У цілому, модифіковані механізм і криптографічний протокол 5.2.2 можуть застосовуватись для взаємної автентифікації користувача, що використовує електронний ключ, з РС і встановлення секретного ключа з підтвердженням для криптотунелю між електронним ключем користувача та модулем захисту РС, цей ключ також може або повинен використовуватись як ключ криптотунелю.

7. Основними недоліками криптографічного протоколу автентифікації та встановлення ключів РС і користувача з електронним ключем згідно з ДСТУ ISO/IEC 15946-3, що знижують можливість його застосування, є відсутність неформального механізму захисту від атаки «Повтор» на одного та декількох перевірників, а також необхідність використання криптографічної контрольної суми із симетричними ключами (ці ключі необхідно також встановлювати), у цьому випадку не забезпечується криптоживучість, тощо.

8. Основними недоліками криптографічного протоколу автентифікації та встановлення ключів РС і користувача з електронним ключем згідно з ДСТУ ISO/IEC 11770-3, що знижують можливість його застосування, є те, що протокол автентифікації РС і користувача, згідно з ДСТУ ISO/IEC 11770-3, поданий у параграфі 4.3, задається формально, не забезпечує в явному вигляді взаємну автентифікацію пред'явника та перевірника, а також необхідність використання криптографічної контрольної суми із симетричними ключами (ці ключі необхідно також встановлювати), у цьому випадку не забезпечується криптоживучість, тощо.

6.11. КРИПТОГРАФІЧНІ ПРОТОКОЛИ АВТЕНТИФІКАЦІЇ РОБОЧИХ СТАНЦІЙ І СЕРВЕРІВ ЗАСТОСУВАНЬ ІЗ СЕРВЕРОМ БЕЗПЕКИ НА ОСНОВІ ЕЦП

6.11.1. Аналіз криптографічних механізмів взаємної автентифікації об'єктів і встановлення ключів між робочими станціями та серверами застосувань із сервером безпеки на основі ЕЦП

Механізми взаємної автентифікації забезпечують виконання перевірки автентичності (справжності) сторін, що взаємодіють або мають наміри взаємодіяти. Стандарт ДСТУ ISO/IEC 9798-3 регламентує три механізми взаємної автентифікації: два з них послідовні – це двопрохідний і трьохпрохідний механізми, і паралельний двопрохідний механізм. Послідовні механізми взаємної автентифікації є адаптованими механізмами однобічної автентифікації. В обох випадках

це потребує одного додаткового обміну й додатково двох кроків. Удосконалення наведених протоколів забезпечує аналогічну стійкість і рівень безпеки. Як базовий варіант взаємної автентифікації між РС та модулем автентифікації й серверами оберемо механізм взаємної паралельної автентифікації з двома паралельними проходами. Такий вибір пояснюється дуже важливою вимогою оперативного здійснення взаємної автентифікації.

Механізм взаємної автентифікації, що розглядається, здійснюється паралельно та ґрунтується на двох двопрохідних механізмах однобічної автентифікації. Паралельне виконання протоколу дозволяє зменшити час його виконання, оскільки він здійснюється паралельно. Реалізація протоколу подана на рис. 6.24.

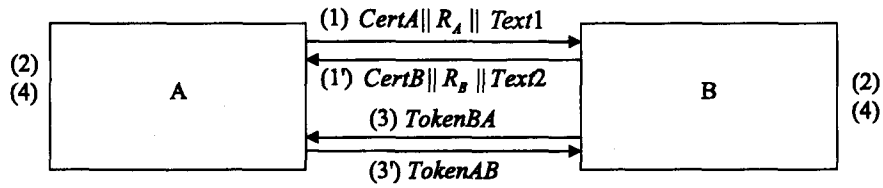

Рис. 6.24. Взаємна паралельна автентифікація з двома проходами

Форма маркерів подана таким чином:

$$TokenAB = R_A \| R_B \| B \| Text4 \| sS_A(R_A \| R_B \| B \| Text3), \quad (6.30)$$

$$TokenBA = R_B \| R_A \| A \| Text6 \| sS_B(R_B \| R_A \| A \| Text5). \quad (6.31)$$

Для формування маркера об'єкти A та B використовують запити на перевірку пароля R_B об'єкта B та R_A об'єкта A, розпізнавальні ідентифікатори об'єктів A та B разом із формуванням підписів $sS_A(R_A \| R_B \| B \| Text3)$, $sS_B(R_B \| R_A \| A \| Text5)$ від заявлених даних $Text3$, $Text5$, значень R_A, R_B та розпізнавальних ідентифікаторів A та B.

Механізм, поданий на рис. 6.24, покроково описується таким чином.

1. Об'єкт A надсилає випадкове число R_A та (не обов'язково) свій сертифікат і $Text1$ об'єкту B.

2. Об'єкт B надсилає випадкове число R_B та (не обов'язково) свій сертифікат і $Text2$ об'єкту A.

3. Обидва об'єкти A та B впевнюються в тому, що володіють дійсним відкритим ключем іншого об'єкта за допомогою або сертифіката, або будь-яких інших засобів.

4. Об'єкт A надсилає маркер $TokenAB$ об'єкту B.

5. Об'єкт B надсилає маркер $TokenBA$ об'єкту A.

6. Обидва об'єкти A та B виконують такі кроки:

а) перевіряють цифровий підпис, що міститься у маркері;

б) перевіряють відповідність випадкового числа, що було перед тим надіслане іншому об'єкту, та випадкового числа, що міститься в підписаних даних маркера.

Цей механізм використовує запит на перевірку пароля R_B об'єкта B, запит на перевірку пароля R_A об'єкта B, загальні характеристики обраних перевірників B та A, заявлену ІА як $Text3$ для об'єкта A і $Text5$ для об'єкта B, яка схована від порушника. За класифікацією вразливостей механізмів автентифікації, поданих у стандарті ISO/IEC 10181-2, цей механізм підпадає під клас 4 «Механізми,

що захищені від розкриття заявленої ІА та атак типу «Повтор» на одного та різних «перевірників», проміжний клас 4*b* «Механізми із запитом пароля». Стійкість такого механізму автентифікації до атак типу «Повтор» та «Підміна» ґрунтується на стійкості двопрохідного механізму однобічної автентифікації.

Додатково необхідно звернути увагу на необхідність включення випадкового числа R_A в підписані дані маркера *TokenAB*, що спрямовано на запобігання атаці, у ході якої об'єкт B може до початку механізму автентифікації отримати цифровий підпис об'єкта A, для даних, які обрано об'єктом B. Цей засіб захисту може знадобитися у випадку, коли об'єкт A використовує свій ключ автентифікації не тільки для здійснення автентифікації об'єктів. З такою самою метою R_B включено до маркера *TokenBA*.

Залежно від часу отримання повідомлень, відправлених на кроках (1) та (2), одна зі сторін може знати випадкове число іншої сторони в той час, коли обирає своє випадкове число. Якщо це небажано, обидві сторони можуть вставити додаткове випадкове число R'_A та R'_B в підписані дані й текстове поле *Text*4 маркера *TokenAB*, у підписані дані й текстове поле *Text*6 маркера *TokenBA* відповідно.

Включення маркеру в перші повідомлення цього механізму автентифікації дозволяють підвищити швидкість процесу автентифікації шляхом здійснення перевірки сертифікатів уже на першому кроці відносно двопрохідного механізму однонаправленої автентифікації, що наведено вище.

Для встановлення взаємної автентифікації цей механізм використовує два проходи для передавання обмінної ІА, яка може містити унікальні числа, представлені позначками часу T_A та T_B, або порядкові номери N_A та N_B відповідно, унікальні характеристики обраних перевірників, представлених розпізнавальним ідентифікатором B для першого проходу та розпізнавальним ідентифікатором A для другого проходу, заявленою ІА об'єкта A, представленою тестовим полем *Text*1, та заявленою ІА об'єкта B, представленою текстовим полем *Text*3. Заявлена ІА захищена від порушника. У цілому, за класифікацією вразливостей механізмів автентифікації, які представлено в стандарті ISO/IEC 10181-2, цей механізм підпадає під клас 4 «Механізми, що захищені від розкриття заявленої ІА та атак типу «Повтор» на одного та різних «перевірників», проміжний клас 4*a* «Механізми з унікальним числом».

Для протистояння атаці типу «Повтор» також використовується цифровий підпис для надання послуги цілісності від даних автентифікації та позначок часу або порядкових номерів. Для синхронізації часу необхідно використовувати систему загальної координації часу.

Для реалізації атаки типу «Підміна» порушнику необхідно підробити підпис від нового значення унікального числа та заявленої ІА. Згідно з потребами стійкості до підробок асиметричних цифрових підписів, що рекомендується використовувати з даним механізмом автентифікації, складність підробки цифрового підпису повинна носити експонентний характер.

Цей механізм можна використовувати разом із протоколами встановлення та розподілення ключів, що наведено в стандарті ISO/IEC 11770-2, 3 для управління ключовою інформацією. Наприклад, для встановлення секретного ключа з підтвердженням та взаємної автентифікації, де ініціатором є пред'явник, можна цей механізм представити таким чином.

Об'єкт B одержує маркер $TokenAB$, перевіряє його та формує за допомогою криптографічної контрольної функції v та ключа K_{AB} секретний ключ

$$K = v_{K_{AB}}\left(\begin{matrix}T_A\\N_A\end{matrix} \| B \| sS_A\left(\begin{matrix}T_A\\N_A\end{matrix} \| B \| Text1\right)\right), \tag{6.32}$$

та зашифровує на цьому ключі маркер $TokenBA$

$$TokenBA = e_K\left(\begin{matrix}T_B\\N_B\end{matrix} \| A \| Text4 \| sS_B\left(\begin{matrix}T_B\\N_B\end{matrix} \| A \| Text3\right)\right). \tag{6.33}$$

Об'єкт A одержує з маркера, що сформовано на першому проході, необхідні дані, виробляє ключ K та розшифровує одержаний маркер $TokenBA$. А далі робить усі перевірки для даного механізму, як це описано вище.

Таким чином, модифікований механізм може проводити взаємну автентифікацію та встановлення секретного ключа з підтвердженням.

Необхідність існування третьої довірчої сторони продиктована необхідністю одержання перевірником B перевірочної ІА для перевірки цифрового підпису sS_A, а також одержання та перевірки статусу сертифіката пред'явника A для першого проходу. І навпаки, для об'єктів B як пред'явника та A як перевірника на другому проході. Управління сертифікатами відкритих ключів покладається на уповноваженого на сертифікацію, наприклад PKI. Розподіл перевірочної ІА покладається на уповноваженого домену безпеки, в якому знаходиться пред'явник. При цьому уповноважений домену безпеки може використовуватися в інтерактивній або автономній автентифікації. В інтерактивному режимі автентифікації уповноважений домену використовується пред'явником для генерування обмінної ІА, а перевірником – для підтримки його у перевірці обмінної ІА. В автономному режимі уповноважений домену безпеки завчасно генерує та розподіляє сертифікати автономної автентифікації, які пізніше використовуються перевірником для підтвердження обміну при автентифікації.

6.11.2. Аналіз криптографічних механізмів взаємної автентифікації обєктів та встановлення ключів між робочими станціями та серверами застосувань із серверами безпеки згідно з ДСТУ ISO/IEC 15946-3

На основі аналізу й досліджень для автентифікації РС і серверів застосувань із сервером безпеки пропонується застосовувати протокол узгодження ключів типу Діффі-Геллмана 5.5 із [213].

6.11.2.1. Сутність протоколу узгодження ключів типу Діффі-Геллмана

Протокол узгодження ключів забезпечує встановлення розділеної таємниці між суб'єктами A та B за два обміни повідомленнями.

Налаштування

Перед процесом узгодження розділеної таємниці (ключа) додатково до спільної інформації необхідно:

– для кожного суб'єкта X установити особистий ключ для узгодження ключів d_x та відкритий ключ для узгодження ключів P_X, який є точкою еліптичної

кривої та для якого виконується рівність $P_X = d_X G$ (цей особистий ключ є ключем цифрового підпису);

– для кожного суб'єкта забезпечити доступ до автентичної копії (сертифіката) відкритого ключа для узгодження ключів іншої сторони.

Кожен суб'єкт повинен незалежно перевірити, що відкритий ключ іншого суб'єкта дійсно є точкою еліптичної кривої [30–32].

6.11.2.2. Механізм автентифікації

Формування маркера ключа (A). Суб'єкт A випадково генерує таємне значення r_A, що належить діапазону $\{1, \ldots n-1\}$, обчислює $r_A G$, формує маркер ключа

$$KT_{A1} = r_A G \tag{6.34}$$

та надсилає його суб'єкту B.

Формування маркера ключа (B). Суб'єкт B випадково генерує таємне значення r_B, що належить діапазону $\{1, \ldots n-1\}$, обчислює $r_B G$, формує маркер ключа

$$KT_{B1} = r_B G \tag{6.35}$$

та надсилає його суб'єкту A.

Формування ключа (A). Суб'єкт A повинен перевірити, що маркер KT_{B1} дійсно є точкою еліптичної кривої [3]. Суб'єкт A обчислює спільну таємницю

$$K_{AB} = (d_A \cdot l)\,(h\,KT_{B1}) \,\|\, (r_A \cdot l)\,(hP_B) \tag{6.36}$$

Формування ключа (B). Суб'єкт B повинен перевірити, що маркер KT_{A1} дійсно є точкою еліптичної кривої [30–32]. Суб'єкт B обчислює розділену таємницю

$$K_{AB} = (r_B \cdot l)\,(h\,P_A) \,\|\, (d_B \cdot l)\,(hKT_{A1}) \tag{6.37}$$

6.11.2.3. Аналіз протоколу узгодження ключів типу Діффі-Геллмана з двома ключовими парами

Протокол 5.5 із [36, 37], наведений вище, має такі властивості та характеристики:

а) забезпечується взаємна автентифікація об'єктів, що взаємодіють;

б) число обмінів повідомленнями – 2;

в) забезпечується криптоживучість ключів суб'єктів A і B окремо;

г) забезпечується взаємна неявна автентифікація ключа.

Таким чином, протокол що аналізується, забезпечує одночасно взаємну автентифікацію суб'єктів і ключів, установлення спільної таємниці та ключів, а також криптоживучість ключів.

1. *Обсяг попередньо необхідної інформації.* Попередньо має бути встановлена загальна інформація згідно [30–32], сформовані пари особистий/ відкритий ключ d_a, Q_a та d_b, Q_b користувачів A та B відповідно, а також сертифіковані відкриті ключі P_a, P_b, що мають бути доступними, із забезпеченням їх цілісності й справжності.

2. *Число проходів.* Алгоритм вимагає виконання двох проходів при встановленні спільного ключа. Криптоаналітик може визначити факт встановлення спільного ключа й перехопити відкриті сеансові ключі ініціатора та відповідача протоколу.

3. *Кількість ключів (ключових пар).* Для виконання протоколу необхідно, щоб обидва суб'єкти мали по одній парі особистий/ відкритий ключ, що генеровані на етапі попередньої підготовки та доставлені суб'єктам з додержанням цілісності

й справжності чи розміщені як доступний сертифікат, а також по одній парі особистий/ відкритий ключ, що мають бути генеровані під час виконання протоколу. Загальна кількість ключових пар, що використовуються під час виконання алгоритму, дорівнює чотирьом.

4. *Додаткова інформація.* Протокол не потребує узгодження додаткової інформації, як таємної, так і відкритої.

5. *Пасивна атака.* Під час цієї атаки криптоаналітик намагається перехопити всі повідомлення, якими обмінюються суб'єкти, що узгоджують ключ. При використанні інтерактивного протоколу узгодження ключів типу Діффі-Геллмана між сторонами відбувається два раунди передачі даних – суб'єкт-ініціатор і суб'єкт-відповідач передають один одному свої відкриті ключі. Криптоаналітик теоретично може перехопити обидві пари ключів. Окрім того, порушник може отримати статичні відкриті ключі (сертифікати). Для розкриття будь-якої інформації, що буде передаватися з використанням спільної таємниці, порушник має встановити за відомими ключами щонайменше по одному особистому ключу зі статичних і сеансових пар ключів, тобто двічі вирішити завдання типу «Повне розкриття». У випадку, коли результати роботи протоколу (спільна таємниця) ніяк не обробляються та використовуються як ключ у чистому вигляді, криптоаналітику може бути вигіднішим з'ясувати тільки половину ключа, тобто вирішити одне дискретне логарифмічне рівняння. Але визначення особистих ключів сеансових пар суб'єктів не призведе до реалізації атаки типу «Повне розкриття», оскільки визначений порушником особистий ключ більше не буде використовуватись у системі і на основі отриманого ключа можна встановити тільки ключ сеансу, який уже відбувся, і виконати розкриття тільки тієї інформації, що передана на цьому ключі.

6. *Активна атака.* Ця атака вимагає взаємодії між суб'єктами під час узгодження ключів. У протоколі два раунди взаємодії між учасниками протоколу – передача відкритого сеансового ключа суб'єкта-ініціатора суб'єкту-відповідачу та навпаки. Для виконання атаки порушник може здійснити тільки одну атаку: завадити суб'єктам, які взаємодіють, виробити ключ. У такому випадку порушник може перехоплювати й модифіковувати повідомлення. У результаті цього суб'єкти не зможуть виробити однакову спільну таємницю. Виконання атак типу «Об'єкт посередині» чи формування спільної таємниці неможливе, бо ініціатор та відповідач володіють сертифікатами (чи просто цілісними й справжніми копіями) статичних відкритих ключів один одного.

7. *Загальний рівень безпеки щодо визначення спільної таємниці (ключа).* Безпека спільної таємниці (ключа) повністю базується на складності розв'язання дискретного логарифмічного рівняння в групі точок еліптичної кривої. Аналіз протоколу (5.5) показав, що порушник не може видати себе як за ініціатора, так і за відповідача протоколу.

8. *Рекомендації та пропозиції.* Протокол 5.5 [213] може бути використаний, коли необхідно забезпечити взаємну явну автентифікацію об'єктів, ключів P_A та P_B, а також взаємну криптографічну живучість. Протокол забезпечує практичну захищеність від пасивних атак типу «Повне розкриття». Для її здійснення необхідно кожен сеанс розв'язувати завдання типу «Повне розкриття» для визначення сеансового особистого ключа, а також розв'язувати завдання «Повне розкриття» для довгострокового особистого ключа, зв'язаного із сертифікатами. Для захисту від активних

атак типу «Модифікування ключів сеансу» необхідно використовувати завадостійкі канали обміну інформацією. При використанні протоколу забезпечується взаємна криптоживучість і неявна автентифікація суб'єктів, які взаємодіють.

6.11.3. Аналіз криптографічних механізмів взаємної автентифікації обєктів і встановлення ключів між робочими станціями та серверами застосувань із серверами безпеки згідно з ДСТУ ISO/IEC 11770-3

На основі аналізу та досліджень для автентифікації РС і серверу застосувань із сервером безпеки можна застосовувати протокол автентифікації та встановлення ключів 3 із ДСТУ ISO/IEC 11770-3.

6.11.3.1. Сутність протоколу автентифікації та встановлення ключів 3

Протокол 3 забезпечує взаємну неявну автентифікацію ключа з автентифікацією суб'єктом B суб'єкта A та встановлення розділюваного таємного ключа (таємниці) між суб'єктами A та B за один прохід (рис. 6.25).

Повинні виконуватись такі вимоги:

а) суб'єкт A має асиметричну систему підпису (S_A, V_A);

б) суб'єкт B має доступ до автентифікованої копії відкритого перетворення перевіряння V_A.

в) суб'єкт B має систему узгодження ключів з ключами (h_B, p_B);

г) суб'єкт A має доступ до автентифікованої копії відкритого ключа p_B для узгодження ключів суб'єкта B.

д) як TVP має використовуватись або позначка часу, або порядковий номер. Якщо використовується позначка часу, необхідні надійні та синхронізовані таймери; якщо використовується порядковий номер, необхідна можливість підтримання та контролювання двосторонніх лічильників;

е) суб'єкти A і B мають узгоджену криптографічну контрольну функцію f (аналогічну стандартизованій у ISO/IEC 9797) і шлях включання розділюваного таємного ключа K_{AB} як ключа цієї криптографічної контрольної функції.

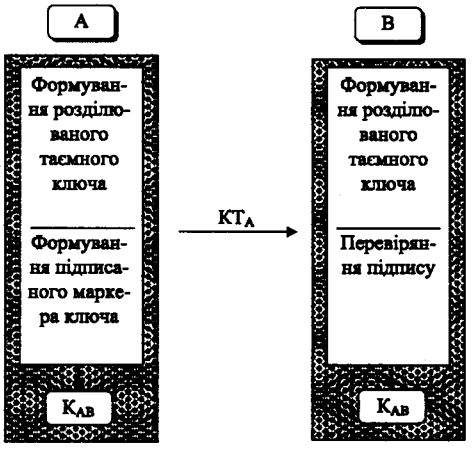

Рис. 6.25. Автентифікація та встановлення ключів, протокол 3

Формування розділюваного таємного ключа (A1.1). Суб'єкт A генерує випадкове таємне число $r \in H$, обчислює $F(r,g)$ та обчислює розділюваний таємний ключ:

$$K_{AB} = F(r, p_B). \tag{6.38}$$

Суб'єкт A, використовуючи розділюваний таємний ключ K_{AB}, обчислює криптографічне контрольне значення $f_{K_{AB}}(A \,||\, TVP)$ шляхом об'єднання свого розрізнювального ідентифікатора та порядкового номера або позначки часу TVP.

Формування підписаного маркера ключа (A1.2). Суб'єкт A підписує криптографічне контрольне значення $f_{K_{AB}}(A \,||\, TVP)$ з використанням свого особистого перетворення підписування S_A. Потім суб'єкт A формує маркер ключа, який складається з його розрізнювального ідентифікатора, вхідного значення $F(r,g)$, TVP, підписаного криптографічного контрольного значення і деяких необов'язкових даних ($Text1$):

$$KT_{A1} = A \,||\, F(r,g) \,||\, TVP \,||\, S_A(f_{K_{AB}}(A \,||\, TVP)) \,||\, Text1 \tag{6.39}$$

і надсилає його суб'єкту B.

Формування розділюваного таємного ключа (B1.1). Суб'єкт B виділяє $F(r,g)$ з одержаного підписаного маркера ключа й обчислює розділюваний таємний ключ, використовуючи свій особистий ключ h_B для узгодження ключів:

$$K_{AB} = F(h_B, F(r,g)). \tag{6.40}$$

Суб'єкт B, використовуючи розділюваний таємний ключ K_{AB}, обчислює криптографічне контрольне значення від розрізнювального ідентифікатора суб'єкта A і TVP.

Перевіряння підпису (B1.2). Суб'єкт B перевіряє підпис суб'єкта A, використовуючи відкрите перетворення перевіряння V_A, а з тим цілісність і справжність одержаного маркера KT_{A1}. Потім суб'єкт B підтверджує оригінальність маркера в часі та своєчасність, аналізуючи TVP.

6.11.3.2. Властивості протоколу автентифікації та встановлення ключів 3

Протокол 3 має такі властивості.

1. Внаслідок використання суб'єктом A особистого ключа ЕЦП забезпечується явна автентифікація суб'єктом B суб'єкта A, внаслідок використання суб'єктом A сертифіката p_B забезпечується встановлення розділюваного таємного ключа (таємниці), і таким чином неявна автентифікація суб'єктом A суб'єкта B.

2. Кожен із суб'єктів впливає на вироблення розділюваного таємного ключа, оскільки кожен із них при його виробленні використовує свій особистий ключ: суб'єкт A – ключ сеансу r, суб'єкт B – статичний ключ h_B, а також відкриті ключі P_B та $F(r, p_B)$ суб'єктів B та A відповідно.

3. Особистий ключ підпису є ключем сеансу, тому він завжди буде новим. Але ініціатором вироблення ключа може бути тільки суб'єкт A.

4. Протокол є однопрохідним, тобто він вимагає передавання відкритого маркера ключа від суб'єкта A суб'єкту B. Суб'єкт A повинен здійснити два асиметричних криптографічних перетворення – для обчислення K_{AB} та при виробленні електронного цифрового підпису. Суб'єкт B також повинен виконати два асиметричних перетворення – при перевірці електронного цифрового підпису та обчисленні розділюваного таємного ключа. Як суб'єкт A, так і суб'єкт B попередні обчислення здійснити не можуть, оскільки розділюваний таємний ключ є сеансовим.

5. Основною вимогою до третьої сторони є виготовлення сертифікатів відкритого ключа P_B та електронного цифрового підпису S_A, а також їх обслуговування протягом життєвого циклу.

6. У протоколі забезпечується неспростовність суб'єкта A, що досягається застосуванням електронного цифрового підпису S_A. Хоча суб'єкт B й застосовує особистий ключ h_B, але при цьому неспростовність B не забезпечується, оскільки розділюваний таємний ключ K_{AB} може обчислити також суб'єкт A.

7. У протоколі забезпечується криптографічна живучість унаслідок використання сеансового ключа r, оскільки він використовується тільки один раз. Компрометація особистого ключа суб'єкта B P_B може призвести до компрометації розділюваного таємного ключа.

8. На протокол можливе здійснення пасивних атак типу «Повне розкриття». Причому повне розкриття особистого сеансового ключа r призводить до компрометації тільки одного розділюваного таємного ключа.

6.11.3.3. Особливості застосування протоколу 3

1. З урахуванням вимог національного законодавства як однонаправлену функцію можна вибрати міждержавний стандарт ГОСТ 34. 311-95 [195] або дозволений Державною службою інший стандарт гешування, наприклад згідно з проектом ДСТУ ISO/IEC 9797-2 [212].

2. Як стандат ЕЦП рекомендуться використати національний стандарт ДСТУ 4145-2002 або дозволений Державною службою інший стандарт. Як альтернативу за наявності відповідного дозволу можуть бути використані алгоритми ЦЕП, що містяться в проекті ДСТУ ISO/IEC 15946-2.

3. Як третю довірчу сторону з виготовлення та обслуговування сертифікатів відкритого ключа P_B обчислення таємниці та електронного цифрового підпису S_A необхідно використовувати послуги спеціалізованого центру сертифікації ключів. Тимчасово можливим є використання послуг комерційного акредитованого центру сертифікації ключів.

4. Для обчислення криптографічних контрольних сум пропонується використовувати криптографічну контрольну функцію f згідно з проектом стандарту ДСТУ ISO/IEC 9797-1 [211]. Ця функція може ґрунтуватися на міждержавному стандарті блокового симетричного шифрування ГОСТ 28147-89 [38] або іншому дозволеному алгоритмі, наприклад FIPS 197, або переможці конкурсу на національний стандарт блокового симетричного шифрування.

6.11.4. Порівняння та вибір криптографічних механізмів взаємної автентифікації об'єктів і встановлення ключів між робочими станціями та сервером застосувань і сервером безпеки

6.11.4.1. Паралельний двопрохідний механізм згідно із стандартом ДСТУ ISO/IEC 9798-3

1. Механізм взаємної паралельної автентифікації з двома паралельними проходами здійснюється паралельно, використовуючи два двопрохідних механізми однобічної автентифікації. Таке виконання протоколу дозволяє зменшити час його здійснення, оскільки він здійснюється паралельно.

2. У цілому, за класифікацією вразливостей механізмів автентифікації, які подано у стандарті ISO/IEC 10181-2, механізм взаємної паралельної автентифікації з двома паралельними проходами, що визначений у ISO/IEC 9798-3, підпадає під клас 4 «Механізми, що захищені від розкриття заявленої ІА та атак типу «Повтор» на одного та різних перевірників», проміжний клас 4*а* «Механізми з унікальним числом». Для протистояння атаці типу «Повтор» використовується електронний цифровий підпис, що забезпечує надання послуги цілісності від даних автентифікації та позначок часу або порядкових номерів. Механізм і протокол забезпечує захист від атаки типу «Підміна», оскільки для її здійснення необхідно вирішити експоненційно складне завдання вирішення дискретного логарифму в групі точок еліптичної кривої.

3. Механізм взаємної паралельної автентифікації з двома паралельними проходами, що наведений у 5.1, здійснюється паралельно, його можна використовувати разом із протоколами встановлення та розподілення ключів, що наведено в стандарті ISO/IEC 11770-2, 3 для управління ключовою інформацією. Паралельне виконання протоколу дозволяє зменшити час його виконання, оскільки він здійснюється паралельно.

4. Включення маркера в перші повідомлення механізму паралельної автентифікації згідно зі стандартом ISO/IEC 9798-3 дозволяють підвищити швидкість процесу автентифікації шляхом здійснення перевірки сертифікатів уже на першому кроці відносно двопрохідного механізму однонаправленої автентифікації, що наведено вище.

5. Необхідність існування третьої довірчої сторони продиктована необхідністю одержання перевірником B перевірочної ІА для перевірки цифрового підпису sS_A, а також одержання та перевірки статусу сертифіката пред'явника A для першого проходу. І навпаки, для об'єктів B як пред'явника та A як перевірника на другому проході. Управління сертифікатами відкритих ключів покладається на уповноваженого на сертифікацію, наприклад PKI. Розподіл перевірочної ІА покладається на уповноваженого домену безпеки, у якому знаходиться пред'явник.

6.11.4.2. Протокол узгодження ключів та автентифікації типу Діффі-Геллмана (протокол 5.5) згідно з ДСТУ ISO/IEC 15946-3

1. Протокол 5.5 із ДСТУ ISO/IEC 15946-3 [36, 37] у загальному вигляді має такі властивості та характеристики:

а) при його застосуванні забезпечується взаємна автентифікація об'єктів, що взаємодіють;

б) число обмінів повідомленнями – 2;

в) забезпечується криптоживучість ключів суб'єктів A і B окремо;

г) забезпечується взаємна неявна автентифікація ключа.

Таким чином, протокол що аналізується, забезпечує одночасно взаємну автентифікацію суб'єктів і ключів, установлення спільної таємниці та ключів, а також криптоживучість ключів.

2. Попередньо повинна бути встановлена загальна інформація, сформовані пари особистий/ відкритий ключ d_a, Q_a та d_b, Q_b користувачів A та B відповідно, а також сертифіковані та доступні із забезпеченням їх цілісності й справжності відкриті ключі P_a, P_b.

3. Для виконання протоколу необхідно, щоб обидва суб'єкти мали по одній парі особистий/ відкритий ключ, які генеровані на етапі попередньої підготовки та доставлені суб'єктам з додержанням цілісності й справжності або розміщені як доступний сертифікат, а також по одній парі особистий/ відкритий ключ, що мають бути згенеровані під час виконання протоколу. Загальна кількість ключових пар, що використовуються під час виконання алгоритму, дорівнює чотирьом.

4. *Захищеність від пасивних атак.* Під час таких атак криптоаналітик намагається перехопити всі повідомлення, якими обмінюються суб'єкти, що узгоджують ключ. При використанні інтерактивного протоколу узгодження ключів типу Діффі-Геллмана між сторонами відбувається два раунди передачі даних – суб'єкт-ініціатор і суб'єкт-відповідач передають один одному свої відкриті ключі. Криптоаналітик теоретично може перехопити обидві пари ключів. Крім того, порушник може отримати статичні відкриті ключі (сертифікати). Для розкриття будь-якої інформації, що буде передаватись з використанням спільної таємниці, порушник має встановити за відомими ключами щонайменше по одному особистому ключу зі статичних і пар ключів сеансу, тобто двічі вирішити завдання типу «Повне розкриття». У випадку, коли результати роботи протоколу (спільна таємниця) ніяк не обробляються та використовуються як ключ у чистому вигляді, криптоаналітику може бути вигіднішим з'ясувати тільки половину ключа, тобто вирішити одне дискретне логарифмічне рівняння. Але визначення особистих ключів сеансових пар суб'єктів не призведе до реалізації атаки типу «Повне розкриття», оскільки визначений порушником особистий ключ більше не буде використовуватись у системі, і на основі отриманого ключа можна встановити тільки ключ сеансу, який уже використаний, і виконати розкриття тільки тієї інформації, що передана на цьому ключі.

5. *При здійсненні активних атак* необхідна взаємодія між суб'єктами під час узгодження ключів. У протоколі два раунди взаємодії між учасниками протоколу – передача відкритого сеансового ключа суб'єкта-ініціатора суб'єкту-відповідачу та навпаки. Для виконання атаки порушник може здійснити тільки одну атаку: завадити суб'єктам, які взаємодіють, виробити ключ. У такому випадку порушник може перехоплювати та модифіковувати повідомлення. У результаті цього суб'єкти не зможуть виробити однакову спільну таємницю. Виконання атак типу «Об'єкт посередині» чи формування спільної таємниці неможливе, бо ініціатор і відповідач володіють сертифікатами (чи просто цілісними й справжніми копіями) статичних відкритих ключів один одного.

6. Протокол 5.5 може бути використаний, коли необхідно забезпечити взаємну явну автентифікацію об'єктів, ключів P_A та P_B, а також взаємну криптографічну живучість. Протокол забезпечує практичну захищеність від пасивних атак типу «Повне розкриття». Для її здійснення необхідно кожен сеанс розв'язувати завдання типу «Повне розкриття» для визначення сеансового особистого ключа, а також розв'язувати завдання «Повне розкриття» для довгострокового особистого ключа, зв'язаного із сертифікатами. Для захисту від активних атак типу «модифікування ключів сеансу» необхідно використовувати завадостійкі канали обміну інформацією. При використанні протоколу забезпечується взаємна криптоживучість і неявна автентифікація суб'єктів, які взаємодіють.

6.11.4.3. Протокол автентифікації та встановлення ключів 3 із ДСТУ ISO/IEC 11770-3

1. Протокол 3 із ДСТУ ISO/IEC 11770-3 [21, 22] забезпечує взаємну неявну автентифікацію ключа з автентифікацією суб'єктом B суб'єкта A та встановлення розділюваного таємного ключа (таємниці) між суб'єктами A і B за один прохід.

2. Внаслідок використання суб'єктом A особистого ключа ЕЦП забезпечується явна автентифікація суб'єктом B суб'єкта A, а внаслідок використання суб'єктом A сертифіката p_B, встановлення розділюваного таємного ключа (таємниці) забезпечується неявна автентифікація суб'єктом A суб'єкта B.

3. Кожен із суб'єктів впливає на вироблення розділюваного таємного ключа, оскільки кожен із них при його виробленні використовує свій особистий ключ: суб'єкт A – ключ сеансу r, суб'єкт B – статичний ключ h_B, а також відкриті ключі P_B та $F(r, g)$ суб'єктів B та A відповідно.

4. Особистий ключ сеансу має бути таємним і він завжди буде новим. Але ініціатором вироблення ключа може бути тільки суб'єкт A.

5. Протокол є однопрохідним, тобто він вимагає передавання відкритого маркера ключа від суб'єкта A суб'єкту B. Суб'єкт A повинен здійснити два асиметричних криптографічних перетворення – для обчислення K_{AB} та при виробленні електронного цифрового підпису. Суб'єкт B також повинен виконати два асиметричних перетворення – при перевірці електронного цифрового підпису та обчисленні розділюваного таємного ключа. Як суб'єкт A, так і суб'єкт B попередні обчислення здійснити не можуть, оскільки розділюваний таємний ключ є ключем сеансу.

6. Основною вимогою до третьої сторони є виготовлення сертифікатів відкритого ключа P_B та електронного цифрового підпису S_A, а також їх обслуговування протягом життєвого циклу.

7. У протоколі забезпечується неспростовність суб'єкта A, що досягається застосуванням електронного цифрового підпису S_A. Хоча суб'єкт B й застосовує особистий ключ h_B, але при цьому неспростовність B не забезпечується, оскільки розділюваний таємний ключ K_{AB} може обчислити також суб'єкт A.

8. Внаслідок використання сеансового ключа r у протоколі забезпечується його криптографічна живучість, тому що він використовується тільки один раз. Компрометація особистого ключа суб'єкта B P_B може призвести до компрометації розділюваного таємного ключа.

9. На протокол можливо здійснення пасивних атак типу «Повне розкриття». Причому повне розкриття особистого сеансового ключа r призводить до компрометації тільки одного розділюваного таємного ключа. При використанні ЕЦП згідно з ДСТУ 4145-2002 складність розв'язання задачі повного розкриття носить експонентний характер.

Результати порівняння та вибору криптографічних механізмів взаємної автентифікації об'єктів і встановлення ключів між робочою станцією та сервером і сервером безпеки

1. Наведені в 5.4.1–5.4.3 результати порівняння та вибору криптографічних механізмів взаємної автентифікації об'єктів і встановлення ключів між РС, сервером застосувань і сервером безпеки (застосувань) дозволяють вибрати як механізм автентифікації та, за необхідності, встановлення ключів (наприклад, для криптотунелів) механізм і на його основі протокол взаємної автентифікації з

двома паралельними чи послідовними проходами згідно з ДСТУ ISO/IEC 9798-3 та електронним цифровим підписом згідно з ДСТУ 4145-2002.

2. На відміну від механізмів (протоколів), що наведені в 6.11.2 та 6.11.3, вибраний механізм забезпечує мінімізацію складності асиметричного перетворення в групі точок еліптичних кривих – необхідно виконати одне асиметричне перетворення типу «електронний цифровий підпис». У той же час при виконанні протоколу, що наведений у 6.11.2, необхідно виконати 3 асиметричних криптоперетворення в групі точок еліптичних кривих з кофакторним множенням, а для протоколу 6.11.3 обов'язково 2.

Окрім того, при застосуванні вибраного протоколу забезпечується явна взаємна автентифікація. У той же час у протоколі 6.11.2 для одного з об'єктів забезпечується тільки неявна автентифікація, а в протоколі 6.11.3 тільки одностороння автентифікація.

3. З урахуванням національних вимог як стандарт електронного цифрового підпису в криптографічному протоколі автентифікації необхідно використовувати національний стандарт ДСТУ 4145-2002. За необхідності та наявності дозволу Державної служби як електронний цифровий підпис можуть бути використані алгоритми, що представлені в (ДСТУ) ISO/IEC 15946-2.

4. Механізм і на його основі протокол взаємної автентифікації з двома паралельними або послідовними проходами згідно з ДСТУ ISO/IEC 9798-3 підпадає під клас 4 «Механізми, що захищені від розкриття заявленої ІА та атак типу «Повтор» на одного та різних «перевірників», проміжний клас 4*а* «Механізми з унікальним числом». Для протистояння атаці типу «Повтор» використовується електронний цифровий підпис, що забезпечує надання послуги цілісності від даних автентифікації та позначок часу або порядкових номерів. Механізм і протокол забезпечує захист від атаки типу «Підміна», оскільки для її здійснення необхідно вирішити експоненційно складне завдання вирішення дискретного логарифму в групі точок еліптичної кривої.

5. Механізм взаємної паралельної автентифікації з двома паралельними проходами, що наведений у 6.11.1, здійснюється паралельно. Його можна використовувати разом із протоколами встановлення та розподілення ключів, що наведено в стандарті ДСТУ ISO/IEC 11770-2, 3 для управління ключовою інформацією. Паралельне виконання протоколу дозволяє зменшити час його виконання, оскільки він здійснюється паралельно.

6.12. КРИПТОГРАФІЧНІ ПРОТОКОЛИ АВТЕНТИФІКАЦІЇ РОБОЧИХ СТАНЦІЙ ТА ВСТАНОВЛЕННЯ КЛЮЧІВ МІЖ СЕРВЕРАМИ БЕЗПЕКИ РІЗНИХ ЛОМ НА ОСНОВІ ЕЦП

6.12.1. Аналіз і вибір криптографічних механізмів взаємної автентифікації об'єктів і встановлення ключів між серверами безпеки різних ЛОМ згідно з ДСТУ ISO/IEC 9798-3

Механізми взаємної автентифікації забезпечують виконання перевірки автентичності (справжності) сторін, що беруть участь у механізмі. Стандарт ДСТУ ISO/IEC 9798-3 регламентує три механізми взаємної автентифікації: два з них послідовні – це двопрохідний і трьохпрохідний механізми, і паралельний

двопрохідний механізм. Послідовні механізми взаємної автентифікації є адаптованими механізмами однобічної автентифікації. В обох випадках це потребує одного додаткового обміну й додатково двох кроків. Удосконалення наведених протоколів забезпечує аналогічну стійкість та рівень безпеки.

Як базовий варіант взаємної автентифікації між серверами безпеки різних ЛОМ виберемо механізм з двома проходами. Цей механізм автентифікації виконується у два проходи та два кроки і базується на однопрохідному механізмі однобічної автентифікації. На рис. 6.26 показано такий механізм, при цьому ініціатором може бути як об'єкт A, так і об'єкт B. Як зображено на рис. 6.26, на першому проході даного механізму об'єкт A є пред'явником для об'єкта B, який представляє перевірника. На другому проході об'єкт B є пред'явником для об'єкта A, який представляє перевірника.

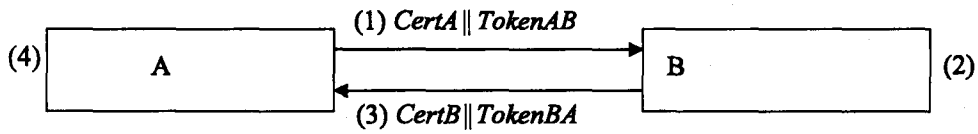

Рис. 6.26. Взаємна автентифікація з двома проходами

Форма маркера ($TokenAB$), що надсилається об'єктом A об'єкту B ідентична формі маркера, визначеного в однопрохідному механізмі однобічної автентифікації:

$$TokenAB = \begin{matrix} T_A \\ N_A \end{matrix} \| B \| Text2 \| sS_A \left(\begin{matrix} T_A \\ N_A \end{matrix} \| B \| Text1 \right). \qquad (6.41)$$

Форма маркера ($TokenBA$), що надсилається об'єктом B об'єкту A:

$$TokenBA = \begin{matrix} T_B \\ N_B \end{matrix} \| A \| Text4 \| sS_B \left(\begin{matrix} T_B \\ N_B \end{matrix} \| A \| Text3 \right). \qquad (6.42)$$

Для формування маркерів $TokenAB$ і $TokenBA$ об'єкти A та B використовують або порядкові номери N_A, N_B відповідно, або позначки часу T_A, T_B відповідно, як змінні в часі параметри формують підписи $sS_A \left(\begin{matrix} T_A \\ N_A \end{matrix} \| B \| Text1 \right)$, $sS_B \left(\begin{matrix} T_B \\ N_B \end{matrix} \| A \| Text3 \right)$ відповідно. $Text1$ і $Text3$ – заявлені дані об'єктів A та B відповідно. Вибір у використанні як змінних в часі параметрів порядкових номерів або позначок часу залежить від технічних можливостей пред'явника та перевірника, а також від оточення.

Механізм, що наведений на рис. 6.26, описується таким чином.

1. Об'єкт A надсилає об'єкту B маркер $TokenAB$, а також (не обов'язково) свій сертифікат.

2. Після отримання повідомлення, що містить $TokenAB$, об'єкт B виконує такі кроки:

а) одержує від уповноваженого на розподілення сертифікатів сертифікат пред'явника A або використовує сертифікат, який надіслано пред'явником. Перевіряє, що має дійсний відкритий ключ пред'явника. Одержує від ТДС перевірочну ІА для заявленої ІА пред'явника;

б) перевіряє коректність маркера $TokenAB$ шляхом:

– перевіряння цифрового підпису, що міститься в маркері, використовуючи перевірочну ІА об'єкта A, позначку часу T_A або порядковий номер N_A, розпізнавальний ідентифікатор B;

– перевіряння коректності позначки часу або порядкового номера;

– порівняння ідентичності значення поля ідентифікатора B у підписаних даних маркера $TokenAB$ та розпізнавального ідентифікатора об'єкта B.

3. Об'єкт B генерує та надсилає маркер $TokenBA$ об'єкту A, а також (не обов'язково) свій сертифікат.

4. Повідомлення крок (3) обробляється аналогічно до кроку (2).

Після отримання повідомлення, що містить $TokenBA$, об'єкт A виконує такі кроки:

а) одержує від уповноваженого на розподілення сертифікатів сертифікат пред'явника B або використовує сертифікат, який надіслано пред'явником. Перевіряє, що має дійсний відкритий ключ пред'явника, одержує від ТДС перевірочну ІА для заявленої ІА пред'явника;

б) перевіряє коректність маркера $TokenBA$ шляхом:

– перевіряння цифрового підпису, що міститься в маркері, використовуючи перевірочну ІА, позначку часу T_B або порядковий номер N_B та розпізнавальний ідентифікатор A;

– перевіряння коректності позначки часу або порядкового номера;

– порівняння ідентичності значення поля ідентифікатора A в підписаних даних маркера $TokenBA$ та розпізнавального ідентифікатора об'єкта A.

Два повідомлення такого механізму пов'язані між собою лише вимогою відносної своєчасності, для подальшого зв'язування цих повідомлень можна використовувати додатково відповідні текстові поля.

Аналіз стійкості кожного проходу цього механізму до атак типу «Підміна» та «Повтор» наведено при розгляді однопрохідного механізму однобічної автентифікації, тому проведемо аналіз щодо можливості протистояння таким атакам для цілісного механізму. Для встановлення взаємної автентифікації даний механізм використовує два проходи для передавання обмінної ІА, яка містить унікальні числа, представлені позначками часу T_A та T_B, або порядкові номери N_A та N_B відповідно, унікальні характеристики обраних перевірників, які представлено розпізнавальним ідентифікатором B для першого проходу, та розпізнавальним ідентифікатором A для другого проходу, заявленою ІА об'єкта A, представленою тестовим полем $Text1$, та заявленою ІА об'єкта B, представленою текстовим полем $Text3$. Заявлена ІА схована від порушника. У цілому, за класифікацією вразливостей механізмів автентифікації, що представлено в стандарті ISO/IEC 10181-2, цей механізм підпадає під клас 4 «Механізми, що захищені від розкриття заявленої ІА та атак типу «Повтор» на одного та різних перевірників», проміжний клас 4*a* «Механізми з унікальним числом».

Для протистояння атаці типу «Повтор» також використовується цифровий підпис для надання послуги цілісності від даних автентифікації та позначок часу або порядкових номерів. Для синхронізації часу необхідно використовувати систему загальної координації часу.

Для реалізації атаки типу «Підміна» порушнику необхідно підробити підпис від нового значення унікального числа та заявленої ІА. Згідно з потребами стійкості до підробок асиметричних цифрових підписів, що рекомендується вико-

ристовувати з даним механізмом автентифікації, складність підробки цифрового підпису має бути не менше ніж експонентною.

Цей механізм можна використовувати разом із протоколами встановлення та розподілення ключів, що наведено в стандарті ISO/IEC 11770-2,3, для управління ключовою інформацією. Наприклад, для встановлення секретного ключа з підтвердженням та взаємної автентифікації, де ініціатором є пред'явник, можна цей механізм подати таким чином.

Об'єкт B одержує маркер $TokenAB$, перевіряє його та формує за допомогою криптографічної контрольної функції ν та ключа K_{AB} секретний ключ

$$K = \nu_{K_{AB}}\left(\begin{matrix}T_A\\N_A\end{matrix} \| B \| sS_A\left(\begin{matrix}T_A\\N_A\end{matrix} \| B \| Text1\right)\right), \tag{6.43}$$

та зашифровує на цьому ключі маркер $TokenBA$:

$$TokenBA = e_K\left(\begin{matrix}T_B\\N_B\end{matrix} \| A \| Text4 \| sS_B\left(\begin{matrix}T_B\\N_B\end{matrix} \| A \| Text3\right)\right). \tag{6.44}$$

Об'єкт A одержує з маркера, що сформовано на першому проході, необхідні дані, виробляє ключ K та розшифровує одержаний маркер $TokenBA$. А далі робить усі перевірки для цього механізму, як описано вище.

Таким чином, модифікований механізм може проводити взаємну автентифікацію та встановлення секретного ключа з підтвердженням.

Необхідність існування третьої довірчої сторони продиктована необхідністю одержання перевірником B перевірочної ІА для перевірки цифрового підпису sS_A, а також одержання та перевірки статусу сертифіката пред'явника A для першого проходу. І навпаки, для об'єктів B як пред'явника та A як перевірника на другому проході. Управління сертифікатами відкритих ключів покладається на уповноваженого на сертифікацію, наприклад PKI. Розподіл перевірочної ІА покладається на уповноваженого домену безпеки, в якому знаходиться пред'явник. При цьому уповноважений домену безпеки може використовуватися в інтерактивній або автономній автентифікації. В інтерактивному режимі автентифікації уповноважений домену використовується пред'явником для генерування обмінної ІА, а перевірником – для підтримки його в перевірці обмінної ІА. В автономному режимі уповноважений домену безпеки в автономному режимі завчасно генерує та розподіляє сертифікати автономної автентифікації, які пізніше використовуються перевірником для підтвердження обміну при автентифікації.

Основним недоліком криптографічного протоколу, що наведений вище, є необхідність розповсюдження та в цілому управління ключами симетричної криптографічної функції на рівні автоматизованої системи 3 рівня (АС-3).

6.12.2. Аналіз та вибір криптографічних механізмів взаємної автентифікації об'єктів і встановлення ключів між серверами безпеки різних ЛОМ згідно з ДСТУ ISO/IEC 11770-3

Для автентифікації серверів різних ЛОМ та встановлення ключів конфіденційного обміну, а також їх автентифікації з метою захисту від НСД розглядається криптографічний протокол 5 (6.5) згідно з ДСТУ ISO/IEC 11770-3.

6.12.2.1. Сутність та аналіз протоколу 5 [21, 22] узгодження ключів та автентифікації

Протокол 5 забезпечує встановлення розділюваного таємного ключа (таємниці) між суб'єктами A і B за два проходи (рис. 6.27). Протокол забезпечує взаємну неявну автентифікацію розділюваного таємного ключа та сумісне управління ключами. Повинні виконуватись такі вимоги:

1) кожен суб'єкт X має особистий ключ $h_X \in H$ для узгодження ключів і відкритий ключ $p_X = F(h_X, g)$ для узгодження ключів;

2) кожен суб'єкт має доступ до автентифікованої копії відкритого ключа для узгодження ключів іншого суб'єкта. Цього можна досягти з використанням протоколів, що наведені в розділі 8;

3) обидва суб'єкта повинні узгодити та використовувати однакову однонаправлену функцію w.

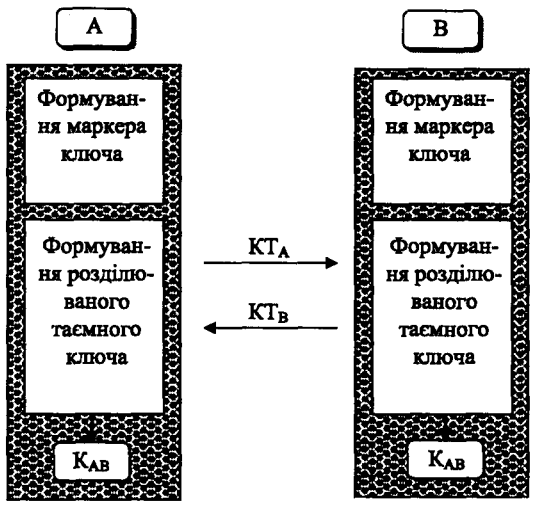

Рис. 6.27. Узгодження ключів, протокол 5

Формування маркера ключа (A1). Суб'єкт A генерує випадкове таємне число $r_A \in H$, обчислює $F(r_A, g)$, формує маркер ключа:

$$KT_{A1} = F(r_A, g) \| Text1 \tag{6.45}$$

і надсилає його суб'єкту B.

Формування маркера ключа (B1). Суб'єкт B генерує випадкове таємне число $r_B \in H$, обчислює $F(r_B, g)$, формує маркер ключа:

$$KT_{B1} = F(r_B, g) \| Text2 \tag{6.46}$$

і надсилає його суб'єкту A.

Формування розділюваного таємного ключа (B2). Суб'єкт B виділяє $F(r_A, g)$ з одержаного маркера ключа KT_{A1} й обчислює розділюваний таємний ключ:

$$K_{AB} = w(F(h_B, F(r_A, g)), F(r_B, p_A)), \tag{6.47}$$

де w є однонаправленою функцією.

Формування розділюваного таємного ключа (А2). Суб'єкт A виділяє $F(r_B,g)$ з одержаного маркера ключа $КТ_{B1}$ й обчислює розділюваний таємний ключ:

$$K_{AB} = w(F(r_A,p_B),F(h_A,F(r_B,g))), \qquad (6.48)$$

де w є однонаправленою функцією.

Результати аналізу дозволяють зробити такі висновки щодо протоколу 5.

1. При кожному узгодженні розділюваного таємного ключа встановлюється новий розділюваний таємний ключ і на основі нього новий таємний ключ. Це досягається за рахунок використання ключів сеансу особистих r_A та r_B, а також відкритих $F(r_A,g)$, $F(r_B,g)$.

2. При узгодженні розділюваного таємного ключа обидва суб'єкти однаковою мірою впливають на обчислення розділюваного таємного ключа, він є залежним як від сеансових, так і від статичних (довгострокових) ключів.

3. Попередньо суб'єкти A та B повинні одержати доступ до сертифікатів відкритих ключів один одного, відповідно P_A та P_B.

4. Попередньо обчислення здійснити не можна, оскільки при кожному обчисленні використовуються сеансові ключі.

5. Протокол ґрунтується на використанні відкритих статичних асиметричних пар ключів, цю функцію може виконувати третя довірча сторона, виготовляючи та забезпечуючи життєвий цикл сертифікатів відкритих ключів відповідно P_A та P_B.

6. З урахуванням рекомендацій міжнародного стандарту ISO/IEC 9594-8 ‖ X-509 ITU, а також закону України «Про електронний цифровий підпис» як відкриті ключі P_A та P_B необхідно використовувати сертифікати вказаних відкритих ключів.

7. При використанні протоколу неспростовність суб'єктів A та B забезпечується за рахунок використання кожним із суб'єктів особистих ключів h_A та h_B і відповідних сертифікатів P_A та P_B.

8. У протоколі 5 забезпечується взаємна криптоживучість розділюваного таємного ключа, що досягається використанням на кожному сеансі пари ключів сеансу r_A та r_B. При цьому компрометація сеансового чи довгострокового ключа (окремо) не призводить до компрометації розділюваного таємного ключа.

9. При записі в полі *Text2* криптографічного контрольного значення на відомих даних, що обчислюється з використанням ключа K_{AB}, протокол забезпечує підтвердження розділюваного таємного ключа суб'єкта A суб'єктом B, а значить, з урахуванням неявної автентифікації – явну автентифікацію розділюваного таємного ключа суб'єктом B суб'єкта A.

10. Забезпечується взаємна неявна автентифікація розділюваного таємного ключа між суб'єктами A та B, а також явна автентифікація розділюваного таємного ключа суб'єктом B суб'єкта A.

11. При використанні протоколу неспростовність суб'єктів A та B забезпечується в неявному вигляді за рахунок використання кожним із суб'єктів особистих ключів h_A та h_B і відповідних сертифікатів p_A та p_B.

12. Проведений аналіз показав, що для обчислення розділюваного таємного ключа порушник (криптоаналітик) повинен щонайменше розв'язати такі задачі (наприклад, через атаку на абонента A):

– одержати сертифікат ключа p_A та розв'язати задачу обчислення відповідного йому особистого ключа h_A;

– перехопити маркер ключа KT_{B1};

– перехопити маркер ключа KT_{A1} та розв'язати задачу обчислення особистого сеансового ключа r_A;

– одержати сертифікат відкритого ключа p_B.

Знаючи односторонню функцію w, обчислити розділюваний таємний ключ K_{AB}.

Таким чином, при здійсненні атаки типу «Повне розкриття» криптоаналітик повинен щонайменше розв'язати дві задачі визначення особистих, статичного (довгострокового) та сеансового ключів, для суб'єкта A – h_A та r_A, для суб'єкта $B - h_B$ та r_B. Ці задачі мають експонентний характер складності (у групі точок еліптичних кривих). При виборі відповідних розмірів параметрів (а вони в стандарті зафіксовані) указані задачі на сучасному етапі розвитку практично не можуть бути розв'язані.

Слід зауважити, що при успішній атаці типу «Повне розкриття» компрометованим буде тільки один розділюваний таємний ключ.

У цілому, протокол 5 узгодження ключів є одним із найбільш захищених, при його використанні забезпечується криптоживучість розділюваного таємного ключа, автентифікація ключів і підтвердження розділюваного таємного ключа, що виробляється. Протокол практично є захищеним від атаки типу «Повне розкриття», оскільки для її здійснення необхідно розв'язати дві експонентно складні задачі (за умови використання криптографічного перетворення в групі точок еліптичних кривих).

Для захисту маркерів від атак типу «Повтор» можна використовувати поля маркерів *Text*1 і *Text*2.

У той же час, при його здійсненні суб'єкти повинні виконувати складні обчислення. Головним же недоліком наведеного протоколу є те, що на першому етапі маркери передаються в незахищеному вигляді, без контролю їх цілісності й автентичності, а також без авторизації джерел формування цих маркерів.

Нижче наводиться комбінований протокол автентифікації, встановлення та підтвердження ключів, що побудований на послідовному використанні двох протоколів – протоколу цифрового підпису маркерів та протоколу 5, що наведений вище в 6.12.2.1.

6.12.3. Розробка вдосконаленого криптографічного протоколу взаємної автентифікації об'єктів і встановлення ключів між серверами безпеки різних ЛОМ

6.12.3.1. Сутність та аналіз перспективного удосконаленого протоколу автентифікації й узгодження ключів

Нижче наводиться комбінований протокол автентифікації та встановлення ключів (спільної таємниці), що побудований на послідовному використанні двох протоколів – протоколу цифрового підпису маркерів та протоколу 5, що наведений вище в 6.12.2.

Удосконалений протокол забезпечує взаємну автентифікацію та встановлення розділюваного таємного ключа між суб'єктами A і B за два проходи. Протокол забезпечує також сумісне управління ключами, встановлення й підтвердження таємниці та ключів, що обумовлено використанням асиметричного цифрового підпису з використанням ДСТУ 4145-20002 та шифрування [219].

Повинні виконуватись такі вимоги:

а) суб'єкт A має асиметричну систему підпису з перетворенням (S_A, V_A);

б) суб'єкт B має асиметричну систему підпису з перетворенням (S_B, V_B);

в) кожен суб'єкт X має особистий ключ $h_X \in H$ для встановлення ключів і відкритий ключ $p_X = F(h_X, g)$ для встановлення ключів;

г) кожен суб'єкт має доступ до автентифікованої копії відкритого ключа для встановлення ключів іншого суб'єкта.

д) обидва суб'єкти повинні узгодити та використовувати одинакові загальносистемні параметри криптографічних перетворень;

е) обидва суб'єкти повинні узгодити та використовувати однакову однонаправлену функцію w.

Формування маркера ключа (A1). Суб'єкт A генерує випадкове таємне число $r_A \in H$, обчислює $F(r_A, g)$, формує маркер ключа та підписує його, використовуючи особистий ключ (перетворення) S_A:

$$KT_{A1} = S_A(F(r_A, g) \| Text1) \tag{6.49}$$

і надсилає його суб'єкту B.

У полі $Text1$ обов'язковими складовими є розрізнювальні ідентифікатори пред'явника та перевірника, а також номери (випадкові числа) або часові мітки захисту від атак типу «Повтор».

У разі використання для здійснення ЕЦП перетворень у групі точок еліптичних кривих [22, 36, 37] над відповідним полем Галуа функція $F(r_A, g)$ має вигляд:

$$F(r_A, g) = r_A G(\mathrm{mod} q),$$

де G – порядок базової точки, q – модуль перетворення.

Формування маркера ключа (B1). Суб'єкт B генерує випадкове таємне число $r_B \in H$, обчислює $F(r_B, g)$, формує маркер ключа та підписує його, використовуючи особистий ключ (перетворення) S_B:

$$KT_{B1} = S_B(F(r_B, g) \| Text2) \tag{6.50}$$

і надсилає його суб'єкту A.

У полі $Text2$ обов'язковими складовими є розрізнювальні ідентифікатори пред'явника та перевірника, а також номери (випадкові числа) або часові мітки захисту від атак типу «Повтор».

У випадку використання для здійснення ЕЦП перетворень у групі точок еліптичних кривих [22, 37] над відповідним полем Галуа функція $F(r_B, g)$ має вигляд:

$$F(r_B, g) = r_B G(\mathrm{mod}\, q), \tag{6.51}$$

де G – порядок базової точки, q – модуль перетворення.

Формування розділюваного таємного ключа (B2). Суб'єкт B перевіряє цілісність і справжність (автентичність) маркера KT_{A1} використовуючи сертифікат відкритого ключа електронного цифрового підпису (перетворення) V_A, потім виділяє $F(r_A, g)$ з одержаного маркера ключа KT_{A1} й обчислює розділюваний таємний ключ (розділювану таємницю):

$$K_{AB} = w(F(h_B, F(r_A, g)), F(r_B, p_A)), \tag{6.52}$$

де w є однонаправленою функцією. З урахуванням вимог національного законодавства як однонаправлену функцію можна вибрати міждержавний стандарт

ГОСТ 34.311-95 або дозволений Державною службою інший стандарт гешування, наприклад, згідно з проектом ДСТУ ISO/IEC 9797-2 [212] або за наявності дозволу ISO/IEC 10118 чи ISO/ IEC 15946-2.

У разі використання при обчисленні розділюваної таємниці перетворень у групі точок еліптичних кривих [22] над відповідним полем Галуа функція $F(h_B, F(r_A, g))$ має вигляд:

$$F(h_B, F(r_A, g)) = h_B \, F(r_A, g) (\text{mod } q), \tag{6.53}$$

де $F(r_A, g)$ – точка еліптичної кривої, що обчислена вище.

Функція $F(r_B, p_A)$ обчислюється у вигляді скалярного добутку і має вигляд:

$$F(r_B, p_A) = r_B p_A (\text{mod } q), \tag{6.54}$$

де p_A – сертифікат відкритого ключа абонента A.

Формування розділюваного таємного ключа (А2). Суб'єкт A перевіряє цілісність і справжність (автентичність) маркера KT_{B1}, використовуючи сертифікат відкритого ключа електронного цифрового підпису (перетворення) V_B, виділяє $F(r_B, g)$ з одержаного маркера ключа KT_{B1} й обчислює розділюваний таємний ключ:

$$K_{AB} = w(F(r_A, p_B), F(h_A, F(r_B, g))), \tag{6.55}$$

де w є однонаправленою функцією.

Аналогічно, як зазначалося вище, як однонаправлену функцію можна вибрати міждержавний стандарт гешування ГОСТ 34.311-95 [41] або дозволений Державною службою інший стандарт гешування, наприклад, згідно з проектом ДСТУ ISO/IEC 9797-2 [212].

У випадку використання при обчисленні розділюваної таємниці перетворень у групі точок еліптичних кривих [21, 22] над відповідним полем Галуа функція $F(h_A, F(r_B, g))$ має вигляд:

$$F(h_A, F(r_B, g)) = h_A F(r_B, g) \, (\text{mod } q), \tag{6.56}$$

де $F(r_B, g)$ – точка еліптичної кривої, що обчислена вище.

Функція $F(r_A, p_B)$ обчислюється у вигляді скалярного добутку і має вигляд

$$F(r_A, p_B) = r_A p_B (\text{mod } q), \tag{6.57}$$

де p_B – сертифікат відкритого ключа абонента B.

Необхідно відзначити, що абоненти A та B при обчисленні розділюваної таємниці K_{AB} повинні узгодити правило об'єднання координат точок еліптичної кривої. Згідно з [22, 36, 213] та додатком A для об'єднання можна використовувати операцію конкатенації координат двох точок в узгодженій послідовності.

Основні властивості вдосконаленого криптографічного протоколу автентифікації та встановлення ключів

Наведений вище вдосконалений протокол автентифікації та встановлення ключів (у подальшому протокол автентифікації та встановленння ключів) між серверами безпеки різних ЛОМ має такі властивості.

1. Завжди забезпечується явна взаємна автентифікація абонентів, що ґрунтується на використанні особистих ключів цифрового підпису та сертифікатів відповідних відкритих ключів іншого абонента при пересиланні підписаних маркерів KT_{A1} і KT_{B1}.

2. Забезпечується цілісність і справжність маркерів $КТ_{A1}$ і $КТ_{B1}$ при їх передаванні та на всіх етапах життєвого циклу, тобто виключається можливість здійснення активних атак на вдосконалений криптографічний протокол (за виключенням атаки типу «Повне розкриття», складність якої має експоненційний характер).

3. При кожному узгодженні розділюваного таємного ключа встановлюється новий розділюваний таємний ключ. Це досягається за рахунок використання ключів сеансу (особистих) r_A та r_B, а також відкритих $F(r_A, g)$, $F(r_B, g)$, які передаються між абонентами із забезпеченням їх цілісності й справжності.

4. При узгодженні розділюваного таємного ключа обидва суб'єкти однаковою мірою впливають на обчислення розділюваного таємного ключа, він є залежним як від сеансових, так і від статичних (довгострокових) ключів.

5. Попередньо суб'єкти A та B повинні одержати доступ до сертифікатів відкритих ключів один одного, відповідно до P_A та P_B встановлення ключів, а також V_A та V_B перевірки електронних цифрових підписів.

6. Попереднє обчислення розділюваної таємниці здійснити неможна, оскільки при кожному обчисленні використовуються сеансові ключі.

7. Протокол ґрунтується на використанні відкритих статичних асиметричних пар P_A та P_B встановлення ключів та електронних цифрових підписів V_A та V_B, цю функцію може виконувати третя довірча сторона, виготовляючи та забезпечуючи життєвий цикл сертифікатів відкритих ключів відповідно P_A та P_B, а також V_A та V_B.

8. З урахуванням рекомендацій міжнародного стандарту ISO/IEC 9594-8 ‖ X-509 ITU, а також закону України «Про електронний цифровий підпис» як відкриті ключі P_A та P_B необхідно використовувати сертифікати відповідно P_A та P_B, а також як відкриті ключі електронного цифрового підпису – сертифікати V_A та V_B згідно з ДСТУ 4145-2002 та ГОСТ 34.311-95.

9. При використанні протоколу неспростовність суб'єктів A та B забезпечується за рахунок використання кожним із суб'єктів особистих ключів h_A та h_B та відповідних сертифікатів P_A та P_B встановлення ключів, а також особистих ключів S_A та S_B електронного цифрового підпису та сертифікатів відкритих ключів електронного цифрового підпису V_A та V_B.

10. У протоколі 5 забезпечується взаємна криптоживучість розділюваного таємного ключа, що досягається використанням на кожному сеансі пари ключів сеансу r_A та r_B. При цьому компрометація сеансового чи довгострокового ключа (окремо) не призводить до компрометації розділюваного таємного ключа.

11. При записі в полі *Text*2 криптографічного контрольного значення на відомих даних, що обчислюється з використанням ключа K_{AB}, протокол забезпечує підтвердження розділюваного таємного ключа суб'єкта A суб'єктом B.

12. Забезпечується взаємна неявна автентифікація розділюваного таємного ключа між суб'єктами A та B, а також явна автентифікація розділюваного таємного ключа суб'єктом B суб'єкта A.

13. Проведений аналіз показав, що для обчислення розділюваного таємного ключа порушник (криптоаналітик) повинен щонайменше розв'язати такі задачі (наприклад, через атаку на абонента A):

– одержати сертифікат ключа p_A та розв'язати задачу обчислення відповідного йому особистого ключа h_A;

– перехопити маркер ключа KT_{B1};

– перехопити маркер ключа KT_{A1} та розв'язати задачу обчислення особистого сеансового ключа r_A;

– одержати сертифікат відкритого ключа p_B.

Знаючи односторонню функцію w можна обчислити розділюваний таємний ключ K_{AB}.

Таким чином, при здійсненні атаки типу «Повне розкриття» криптоаналітик повинен щонайменше розв'язати дві задачі визначення особистих, статичного (довгострокового) та сеансового ключів, для суб'єкта A – h_A та r_A, для суб'єкта B – h_B та r_B. Ці задачі мають субекспоненційний (при перетвореннях у полях та кільцях) або експоненційний характер (у групі точок еліптичних кривих). При виборі відповідних параметрів вони практично не можуть бути вирішеними. Слід зауважити, що при успішній атаці «Повне розкриття» буде скомпрометований тільки один розділюваний таємний ключ.

14. Для встановлення взаємної автентифікації цей механізм використовує два проходи для передавання обмінної ІА, що містить унікальні числа, представлені позначками часу T_A і T_B, або порядкові номери N_A і N_B відповідно, яка представлена в тестових полях *Text*1 і *Text*2. Заявлена ІА захищена від порушника. У цілому, за класифікацією вразливостей механізмів автентифікації, які подано в стандарті ISO/IEC 10181-2, цей механізм підпадає під клас 4 «Механізми, що захищені від розкриття заявленої ІА та атак типу «Повтор» на одного та різних перевірників, проміжний клас 4*a* «Механізми з унікальним числом та цифровим підписом».

15. Для протистояння атаці типу «Повтор» також використовується цифровий підпис для надання послуги цілісності від даних автентифікації та позначок часу або порядкових номерів. Для синхронізації часу необхідно використовувати систему загальної координації часу.

16. Для реалізації атаки типу «Підміна» порушнику необхідно підробити підпис від нового значення унікального числа та заявленої ІА. Згідно з потребами стійкості до підробок асиметричних цифрових підписів, що рекомендується використовувати з таким механізмом автентифікації, складність підробки цифрового підпису повинна бути не менше ніж експонентною.

17. Як цифровий підпис пропонується використовувати алгоритм цифрового підпису ДСТУ 4145:2002, схвалений для застосування з метою захисту інформації, що є власністю Держави, спеціальним уповноваженим органом державного управління у сфері криптографічного захисту інформації.

18. Для забезпечення надійного рівня безпеки при використанні алгоритму цифрового підпису ДСТУ 4145 необхідно забезпечити виконання пропозицій, що регламентують вибір загальних параметрів цифрового підпису та стандартизовані обчислювальні алгоритми генератора випадкових чисел і геш-функції.

19. У стандарті ДСТУ 4145 пропонується використовувати генератор випадкових послідовностей, визначений цим стандартом, або інший генератор випадкових послідовностей, рекомендований уповноваженим органом державної влади

у сфері криптографічного захисту інформації для отримання випадкових цілих чисел, випадкових елементів основного поля та випадкових точок еліптичних кривих.

У цьому стандарті пропонується використовувати геш-функцію, що застосовується для обчислення й перевірки цифрового підпису, визначену в ГОСТ 34.311-95, або будь-яку іншу геш-функцію, рекомендовану уповноваженим органом державної влади у сфері криптографічного захисту інформації.

20. У цілому, розроблений на основі комбінування протоколу електронного цифрового підпису та протоколу 5 встановлення ключів удосконалений протокол автентифікації та встановлення ключів є найбільш захищеним. При його використанні забезпечується явна автентифікація абонентів, неявна автентифікація ключів, криптоживучість розділюваного таємного ключа та, за необхідності, підтвердження розділюваного таємного ключа, що виробляється. Протокол практично є захищеним від атаки типу «Повне розкриття», оскільки для її здійснення необхідно розв'язати дві експоненційно складні задачі.

6.13. УЗАГАЛЬНЕНІ ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ ЩОДО КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ З ЕЦП

1. Механізми автентифікації можуть піддаватися атакам, які обмежують їх ефективність. Механізми автентифікації, які можна використовувати для надання підтримки у фазі передавання, класифікують відносно загроз(и), проти яких ці механізми є невразливими. Механізми базуються на принципі автентифікації при її здійсненні «дещо відомо». Усі наведені механізми можна застосовувати до об'єктів автентифікації, а механізми з цифровим підписом (геш-значенням) можна застосовувати до автентифікації джерела даних.

Основні класи механізмів автентифікації можна визначити таким чином:

Клас 0 – незахищений;

Клас 1 – захищений від розкриття заявленої ІА;

Клас 2 – захищений від розкриття заявленої ІА та атаки типу «Повтор» для різних перевірників;

Клас 3 – захищений від розкриття заявленої ІА та атаки типу «Повтор» на одного перевірника;

Клас 4 – захищений від розкриття заявленої ІА та атаки типу «Повтор» на одного перевірника або різних перевірників.

При використанні функції шифрування як частини генерування для формування ключа використовують заявлену ІА, можливо разом з іншою інформацією. При використанні функції шифрування як частини використовують для формування ключа перевіряння перевірочну ІА, можливо разом з іншою інформацією, яку одержують в обміні при автентифікації.

Спочатку розглядаються обміни при автентифікації з точки зору пред'явника і тому пред'явник завжди є ініціатором. Використовуючи цю точку зору пояснюються всі класи механізмів спрямованої автентифікації, а потім уточнюються для обмінів, де ініціатором є перевірник, для обмінів, які використовуються для однонаправленої та взаємної автентифікації.

2. При виконанні механізму автентифікації здійснюється перевірка дійсності суб'єкта, що робить запит на доступ до інформації чи ресурсів системи за пред'явленим ним ідентифікатором. За такої ознаки під ідентифікатором виступають ознака автентифікації суб'єкта та/чи електронний засіб, наприклад електронний ключ, смарт-карта тощо. Найпростішим механізмом автентифікації є пред'явлення користувачем PIN-коду карти. У цьому випадку PIN-код використовується як для автентифікації користувача, так і для авторизації доступу до інформації чи ресурсів і, таким чином, реалізується найпростіший метод розмежування доступу.

Процес автентифікації користувача у найбільш узагальненому вигляді можна подати в такий спосіб. У процесі здійснення доступу користувач вставляє електронний засіб у спеціальний пристрій (порт), що підключений до робочої станції, і потім вводить свою ознаку автентифікації (пароль, сертифікат відкритого ключа, особистий ключ, біометричну інформацію тощо). Процес автентифікації користувача розпочинається тільки за наявності, у найпростішому випадку, електронного засобу в пристрої зчитування або шляхом порівняння ідентифікатора користувача, уведеного з клавіатури чи іншим чином, з ідентифікатором користувача, що зберігається в ЕЗ. Потім у робочій станції (РС) ознака автентифікації, що введена користувачем, зіставляється з інформацією, що зберігається в ЕЗ. При успішному порівнянні РС надає доступ до інформації та/чи своїх ресурсів і процес автентифікації вважається завершеним.

3. За результатами аналізу й порівняння різних криптографічних механізмів і протоколів визначено необхідність врахування при виборі криптографічних протоколів таких потенційних послуг, характеристик і властивостей:

1) наявність (реалізація) послуги автентифікації об'єкта (процесу), суб'єкта;

2) наявність (реалізація) послуги автентифікації ключа (ключів);

3) вид автентифікації об'єктів (процесів) і суб'єктів;

4) вид автентифікації ключів;

5) наявність послуги встановлення ключа (ключів);

6) наявність послуги підтвердження ключа (ключів);

7) новизна ключа (ключів) на кожному з етапів встановлення ключів;

8) перелік послуг з управління ключами;

9) захищеність від загроз типу «Передача раніше переданого легального повідомлення», типу «Повтор»;

10) захищеність від загроз типу «Маскарад»;

11) захищеність від загроз типу «Модифікація»;

12) криптографічна живучість встановлених ключів;

13) гарантії забезпечення послуг: конфіденційність, цілісність, доступність, справжність (автентичність) і неспростовність щодо інформації автентифікації та ключів;

14) число обмінів при здійсненні криптографічного протоколу;

15) складність виконання криптоаналізу відносно ключів та інформації, що захищається;

16) складність обчислень при здійсненні криптографічного протоколу;

17) можливість виконання попередніх обчислень;

18) наявність та вимоги до третьої довірчої сторони тощо.

4. У таблиці 6.3 подано результати аналізу вразливості та характеристики різних класів і проміжних класів механізмів, розглянутих вище.

За необхідності об'єкти можуть здійснити автентифікацію із залученням щонайменше однієї ТДС. У цьому випадку необхідно визначити реальну довіру між кожним об'єктом та будь-якою ТДС. У такій моделі залучають тільки одну довірчу сторону, причому ТДС може бути розподіленою в просторі. Інші моделі визначають множину третіх ТДС, які довіряють одна одній, причому в загальній моделі залучається множина ТДС, у якій немає довіри одна одній. Залучення декількох ТДС може бути обґрунтованим, якщо необхідно забезпечити резервування послуг третьої довірчої сторони.

5. Наведені в 6.10–6.12 криптографічні протоколи автентифікації, розподілення, встановлення та узгодження забезпечують необхідний рівень захищеності за умови використання в них ЕЦП. Указане дозволяє забезпечити неспростовність відправника на основі використання особистого ключа автентифікації.

Аналіз і порівняння криптографічних механізмів і протоколів автентифікації, що подані в ДСТУ ISO/IEC 9798-3, ДСТУ ISO/IEC 15946-3 та ДСТУ ISO/IEC 11770–3, дозволяє зробити висновок, що як основний механізм та на його основі криптографічний протокол автентифікації РС і користувачів з електронним ключем і встановлення ключів, краще вибрати механізм 5.2.2 взаємної автентифікації із ДСТУ ISO/IEC 9798-3. Протокол 5.2.2 за класифікацією вразливостей механізмів автентифікації згідно з міжнародним стандартом ISO/IEC 10181-2 підпадає під найвищий 4 клас захищеності «Механізми, що захищені від розкриття заявленої ІА та атак типу «Повтор» на одного та різних «перевірників», проміжний клас 4*b* «Механізми із запитом паролю».

Згідно з механізмом 5.2.2 із ДСТУ ISO/IEC 9798-3 під час проходження автентифікації кожен об'єкт підтверджує свою ідентичність шляхом пред'явлення доказу того, що він володіє знанням свого особистого ключа (електронного) цифрового підпису. Цифровий підпис може бути перевірений будь-яким об'єктом, який має доступ до відкритого ключа (сертифіката) електронного цифрового підпису.

З урахуванням національних вимог як стандарт електронного цифрового підпису в криптографічному протоколі автентифікації необхідно використовувати національний стандарт ДСТУ 4145-2002. За необхідності як електронний цифровий підпис можуть бути використані алгоритми, що подані в ISO/IEC 15946-2 (ISO/IEC 14888-3).

Модифіковані механізм і криптографічний протокол 5.2.2 можуть застосовуватись для взаємної автентифікації користувача, що використовує електронний ключ, з РС та встановлення секретного ключа з підтвердженням для криптографічного тунелю між електронним ключем користувача та модулем захисту РС, також цей ключ може або повинен використовуватись як ключ криптографічного тунелю.

6. Вибраний механізм та на його основі протокол взаємної автентифікації з двома паралельними або послідовними проходами згідно з ДСТУ ISO/IEC 9798-3 підпадає під клас 4 «Механізми, що захищені від розкриття заявленої ІА та атак типу «Повтор» на одного та різних «перевірників», проміжний клас 4*a* «Механізми з унікальним числом». Для протистояння атаці типу «Повтор» використовується

електронний цифровий підпис, що забезпечує надання послуги цілісності від даних автентифікації та позначок часу або порядкових номерів. Механізм і протокол забезпечують захист від атаки типу «Підміна», оскільки для її здійснення необхідно вирішити експоненційно складну задачу розв'язання дискретного логарифму в групі точок еліптичної кривої. Цей механізм взаємної паралельної автентифікації з двома паралельними проходами здійснюється паралельно, його можна використовувати разом із протоколами встановлення та розподілення ключів, що наведено в стандарті ДСТУ ISO/IEC 11770-2, 3, для управління ключовою інформацією. Паралельне виконання протоколу дозволяє зменшити час його виконання, оскільки він здійснюється паралельно.

7. Наведений у 6.12 удосконалений протокол автентифікації та встановлення ключів (у подальшому протокол автентифікації та встановлення ключів між серверами безпеки різних ЛОМ) має суттєві переваги перед іншими, у тому числі:

– завжди забезпечується явна взаємна автентифікація абонентів, що ґрунтується на використанні особистих ключів цифрового підпису та сертифікатів відповідних відкритих ключів іншого абонента при пересиланні підписаних маркерів $КТ_{A1}$ і $КТ_{B1}$;

– забезпечується цілісність і справжність маркерів $КТ_{A1}$ і $КТ_{B1}$ при їх передаванні та на всіх етапах життєвого циклу, тобто виключається можливість здійснення активних атак на вдосконалений криптографічний протокол (за виключенням атаки типу «Повне розкриття», складність якої має експоненційний характер);

– при кожному узгодженні розділюваного таємного ключа встановлюється новий розділюваний таємний ключ, що досягається за рахунок використання ключів сеансу (особистих) r_A та r_B, а також відкритих $F(r_A,g)$, $F(r_B,g)$, які передаються між абонентами із забезпеченням їх цілісності та справжності;

– при узгодженні розділюваного таємного ключа обидва суб'єкти однаковою мірою впливають на обчислення розділюваного таємного ключа, він є залежним як від сеансових, так і від статичних (довгострокових) ключів;

– суб'єкти A та B попередньо повинні одержати доступ до сертифікатів відкритих ключів один одного, відповідно до P_A та P_B встановлення ключів, а також V_A та V_B перевірки електронних цифрових підписів;

– удосконалений протокол ґрунтується на використанні відкритих статичних асиметричних пар P_A та P_B встановлення ключів та електронних цифрових підписів V_A та V_B, цю функцію може виконувати третя довірча сторона, виготовляючи й забезпечуючи життєвий цикл сертифікатів відкритих ключів відповідно P_A та P_B, а також V_A та V_B;

– з урахуванням рекомендацій міжнародного стандарту ДСТУ ISO/IEC 9594-8 || X-509 ITU, а також ДСТУ ISO/IEC 15946-3 як відкриті ключі P_A та P_B необхідно використовувати сертифікати відповідно P_A та P_B, а також як відкриті ключі електронного цифрового підпису – сертифікати V_A та V_B;

– при використанні протоколу неспростовність суб'єктів A та B забезпечується за рахунок використання кожним із суб'єктів особистих ключів h_A та h_B і відповідних сертифікатів P_A та P_B встановлення ключів, а також особистих ключів S_A та S_B електронного цифрового підпису та сертифікатів відкритих ключів електронного цифрового підпису V_A та V_B;

– у протоколі забезпечується взаємна криптографічна живучість розділюваного таємного ключа, що досягається використанням на кожному сеансі пари ключів сеансу r_A та r_B, причому компрометація сеансового чи довгострокового ключа (окремо) не призводить до компрометації розділюваного таємного ключа;

– при записі в полі *Text*2 криптографічного контрольного значення на відомих даних, що обчислюється з використанням ключа K_{AB}, протокол забезпечує підтвердження розділюваного таємного ключа суб'єкта *A* суб'єктом *B*;

– забезпечується взаємна неявна автентифікація розділюваного таємного ключа між суб'єктами *A* та *B*, а також явна автентифікація розділюваного таємного ключа суб'єктом *B* суб'єкта *A*;

– для встановлення взаємної автентифікації цей механізм використовує два проходи для передавання обмінної ІА, яка містить унікальні числа, представлені позначками часу T_A і T_B, або порядкові номери N_A та N_B відповідно, яка представлена в тестових полях *Text*1 і *Text*2 . Заявлена ІА захищена від порушника. У цілому, за класифікацією вразливостей механізмів автентифікації, поданих у стандарті ISO/IEC 10181-2, цей механізм підпадає під клас 4 «Механізми, що захищені від розкриття заявленої ІА та атак типу «Повтор» на одного та різних «перевірників», проміжний клас 4*a* «Механізми з унікальним числом» та цифровим підписом;

– для протистояння атаці типу «Повтор» також використовується цифровий підпис для надання послуги цілісності від даних автентифікації та позначок часу або порядкових номерів. Для синхронізації часу необхідно використовувати систему загальної координації часу;

– для реалізації атаки типу «Підміна» порушнику необхідно підробити підпис від нового значення унікального числа та заявленої ІА. Згідно з потребами стійкості до підробок асиметричних цифрових підписів, що рекомендується використовувати з таким механізмом автентифікації, складність підробки цифрового підпису повинна бути не менше ніж експонентною;

– як цифровий підпис пропонується використовувати алгоритм цифрового підпису ДСТУ 4145:2002, схвалений для застосування з метою захисту інформації, що є власністю Держави, спеціальним уповноваженим органом державного управління у сфері криптографічного захисту інформації.

У цілому, розроблений на основі комбінування протоколу електронного цифрового підпису та протоколу встановлення ключів удосконалений протокол автентифікації та встановлення ключів є найбільш захищеним. При його використанні забезпечується явна автентифікація абонентів, неявна автентифікація ключів, криптографічна живучість розділюваного таємного ключа та, за необхідності, підтвердження розділюваного таємного ключа, що виробляється. Протокол практично є захищеним від атаки типу «Повне розкриття», оскільки для її здійснення необхідно розв'язати дві експоненційно складні задачі.