МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ДНІПРОВСЬКА ПОЛІТЕХНІКА»

ІНСТИТУТ ЕЛЕКТРОЕНЕРГЕТИКИ
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

КОНСПЕКТ ЛЕКЦІЙ

з дисципліни «Методи побудови та аналізу криптосистем»

для студентів-магістрів спеціальності 125 Кібербезпека
галузі знань 12 Інформаційні технології

Дніпро
НТУ «ДП»
2019

Саксонов Г.М.

Конспект лекцій з дисципліни «Методи побудови та аналізу криптосистем» для студентів-магістрів спеціальності 125 Кібербезпека галузі знань 12 Інформаційні технології / Упоряд.: Г.М. Саксонов, О.А. Жукова ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2019. – 37 с.

Упорядники:
Г.М. Саксонов, ст. викладач;
О.А. Жукова, доц.

Затверджено методичною комісією зі спеціальності 125 Кібербезпека (протокол № 7 від 07.03.2019) за поданням кафедри безпеки інформації та телекомунікацій (протокол № 7 від 07.03.2019).

Подано конспект лекцій з дисципліни «Методи побудови та аналізу криптосистем» для студентів-магістрів спеціальності 125 Кібербезпека галузі знань 12 Інформаційні технології.

Відповідальний за випуск зав. кафедри БІТ В.І. Корнієнко, д-р техн. наук, проф.

ПЕРЕДМОВА

Основною метою курсу «Методи побудови і аналізу криптосистем» є здобуття теоретичних та практичних знань організації і функціонування надійних систем криптографічного захисту інформації.

Криптографія – до 70-х рр. XX ст. – галузь науки і практичної діяльності, пов'язана з розробкою, застосуванням і аналізом шифросістем. В даний час криптографія – галузь науки, техніки і практичної діяльності, пов'язана з розробкою, застосуванням і аналізом криптографічних систем захисту інформації. Основними функціями криптографічних систем є забезпечення конфіденційності і аутентифікації різних аспектів інформаційної взаємодії. Джерелом загроз при вирішенні криптографічних завдань вважаються навмисні дії противника або несумлінного учасника інформаційної взаємодії, а не випадкові спотворення інформації внаслідок перешкод, відмов і т. п.

Курс «Методи побудови і аналізу криптосистем» може вивчатися як окрема дисципліна, або як складова частина більш загального курсу, яка розкриває варіанти визначення основних криптографічних понять, заснованих на введенні узагальнюючого поняття криптосистеми.

Визначаються види криптографічних систем, основними з яких є системи шифрування, ідентифікації, імітозащіти, цифрового підпису, і ключова система, що забезпечує роботу інших систем.

1. ОСНОВНІ ПОНЯТТЯ І ВИЗНАЧЕННЯ.

Конфіденційність – захищеність інформації від ознайомлення з її змістом з боку осіб, які не мають права доступу до неї.

Аутентифікація – встановлення (тобто перевірка і підтвердження) достовірності різних аспектів інформаційної взаємодії: сеансу зв'язку сторін (ідентифікація), змісту (імітозащіти) і джерела (встановлення авторства) переданих повідомлень, часу взаємодії і т. п., що є важливою складовою частиною проблеми забезпечення достовірності одержуваної інформації. Особливо гостро ця проблема стоїть у разі сторні, що не довіряють один одному, коли джерелом загроз може служити не тільки третя сторона (супротивник), а й сторона, з якої здійснюється інформаційна взаємодія. Рисунок 1.1 ілюструє визначення криптографії і показує її основні складові частини. Пунктирні стрілки показують тісні взаємозв'язки між цими трьома складовими.

1.1. ВИДИ КРИПТОСИСТЕМ

Система криптографічна (криптосистема) – система забезпечення безпеки захищеної мережі, яка використовує криптографи етичні засоби. В якості підсистем може включати системи шифрування, ідентифікації, імітозащіти, цифрового підпису та ін., а також ключову систему, що забезпечує роботу інших систем. В основі вибору і побудови криптосистеми лежить умова забезпечення криптографічного стійкості. Залежно від ключової системи розрізняють симетричні і асиметричні криптосистеми.

Система криптографічна (криптосистема) – система забезпечення безпеки захищеної мережі, яка використовує криптографи етичні засоби. В якості підсистем може включати системи шифрування, ідентифікації, імітозащіти, цифрового підпису та ін., а також ключову систему, що забезпечує роботу інших систем. В основі вибору і побудови криптосистеми лежить умова забезпечення криптографічного стійкості. Залежно від ключової системи розрізняють симетричні і асиметричні криптосистеми [5].

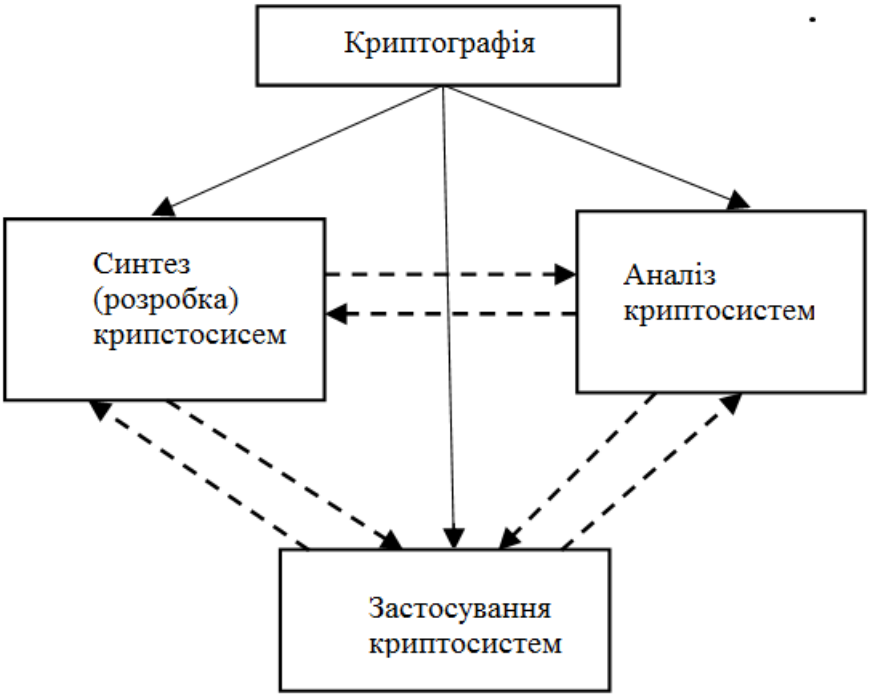

Рис. 1.1. Основні складові частини криптографії.

Засоби криптографічні – в широкому сенсі – методи і засоби забезпечення безпеки інформації, що використовують криптографічні перетворення інформації: у вузькому сенсі – кошти, реалізовані у вигляді документів, механічних, електро-механічних, електронних технічних пристроїв або програм, призначених для виконання функцій криптографічних системи.

Криптографічне перетворення інформації – перетворення інформації з використанням одного з криптографічних алгоритмів визначається цільовим призначенням криптографічної системи. Симетричні криптосистеми – криптосистеми з симетричними (секретними) ключами. Симетричність означає тут, що ключі, які визначають пару взаємно зворотних криптографічних перетворень, можуть бути отримані один з іншого з невеликою трудомісткістю.

Стійкість симетричної криптосистеми визначається трудомісткістю, з якої противник може обчислити будь-який з секретних ключів, і оцінюється при загальноприйнятому допущенні, що противнику відомі всі елементи криптосистеми, за винятком секретного ключа.

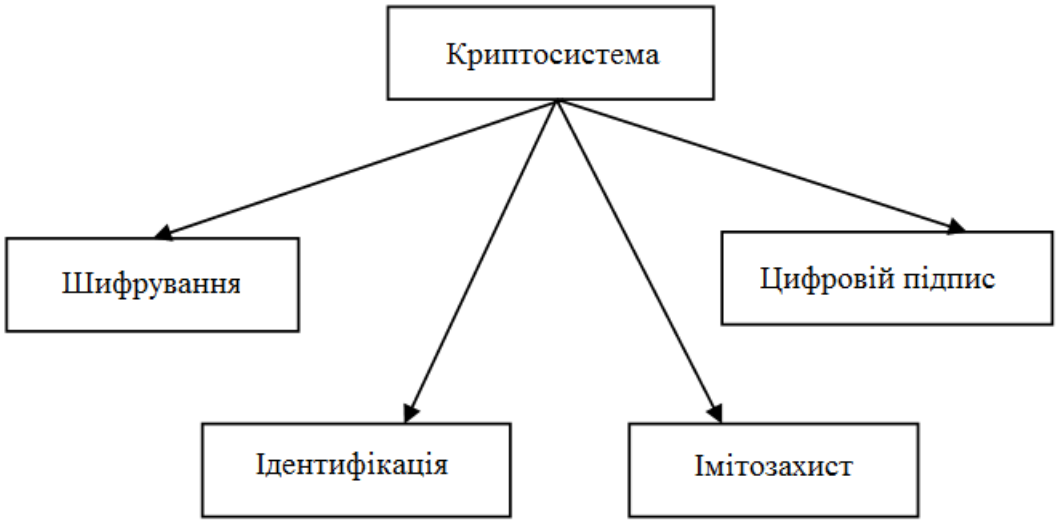

Рис. 1.2. Види криптосистем

Асиметричні криптосистеми – криптосистеми з асиметричними (секретними і відкритими) ключами. Асиметричність означає, що з двох ключів, які задають пару взаємно зворотних криптографічних перетворень, один є секретним, а інший – відкритим. Відкриті ключі відомі всім учасникам захищеної мережі і противнику, але кожен учасник мережі зберігає в таємниці свій секретний ключ. Стійкість асиметричною криптосистеми визначається трудомісткістю, з якої противник може обчислити секретний ключ, виходячи із знання відкритого ключа та іншої додаткової інформації про криптосистему.

Шіфросістема – криптографічна система забезпечення конфіденційності, призначена для захисту інформації від ознайомлення з її змістом осіб, які не мають права доступу до неї, шляхом шифрування інформації. Математична модель шіфросістеми включає спосіб кодування початкової і витікаючої інформації, шифр і ключову систему.

Система імітозащіти (забезпечення цілісності) інформації – криптографічна система, що виконує функцію аутентифікації змісту повідомлення або документа і призначена для захисту від несанкціонованого зміни інформації або нав'язування хибної інформації. Математична модель системи імітозащіти включає криптографічний алгоритм імітозахищенного кодування інформації (алгоритм шифрування, код аутентифікації, або інше

перетворення) і алгоритм прийняття рішення про істинність отриманої інформації, а також ключову систему.

Система ідентифікації – криптографічна система, що виконує функцію аутентифікації сторін у процесі інформаційної взаємодії. Математична модель системи ідентифікації включає протокол ідентифікації і ключову систему.

Система цифрового підпису – криптографічна система, що виконує функцію аутентифікації джерела повідомлення або документа і призначена для захисту від відмови суб'єктів від деяких з раніше скоєних ними дій. Наприклад, відправник може відмовитися від факту передачі повідомлення, стверджуючи, що його створив сам одержувач, а одержувач легко може модифікувати, підмінити або створити нове повідомлення, а потім стверджувати, що воно отримано від відправника. Математична модель системи цифрового підпису включає схему цифрового підпису та ключову систему.

Система ключова (рис. 1.3) – визначає порядок використання криптографічного системи і включає системи установки і управління ключами.

Система установки ключів – визначає алгоритми і процедури генерації, розподілу, передачі і перевірки ключів.

Система управління ключами – визначає порядок використання, зміни, зберігання та архівування, резервного копіювання та відновлення, заміни або вилучення з обігу скомпрометованих, а також знищення старих ключів. Метою управління ключами є нейтралізація таких загроз, як: компрометація конфіденційності секретних ключів, компрометація автентичності секретних або відкритих ключів, несанкціоноване використання секретних або відкритих ключів, наприклад використання ключа, термін дії якого закінчився [3].

Система ключова симетричною криптосистеми – заснована на використанні симетричних (секретних) ключів. Основними проблемами таких систем є побудова системи установки ключів та забезпечення їх збереження для мереж з великим числом абонентів.

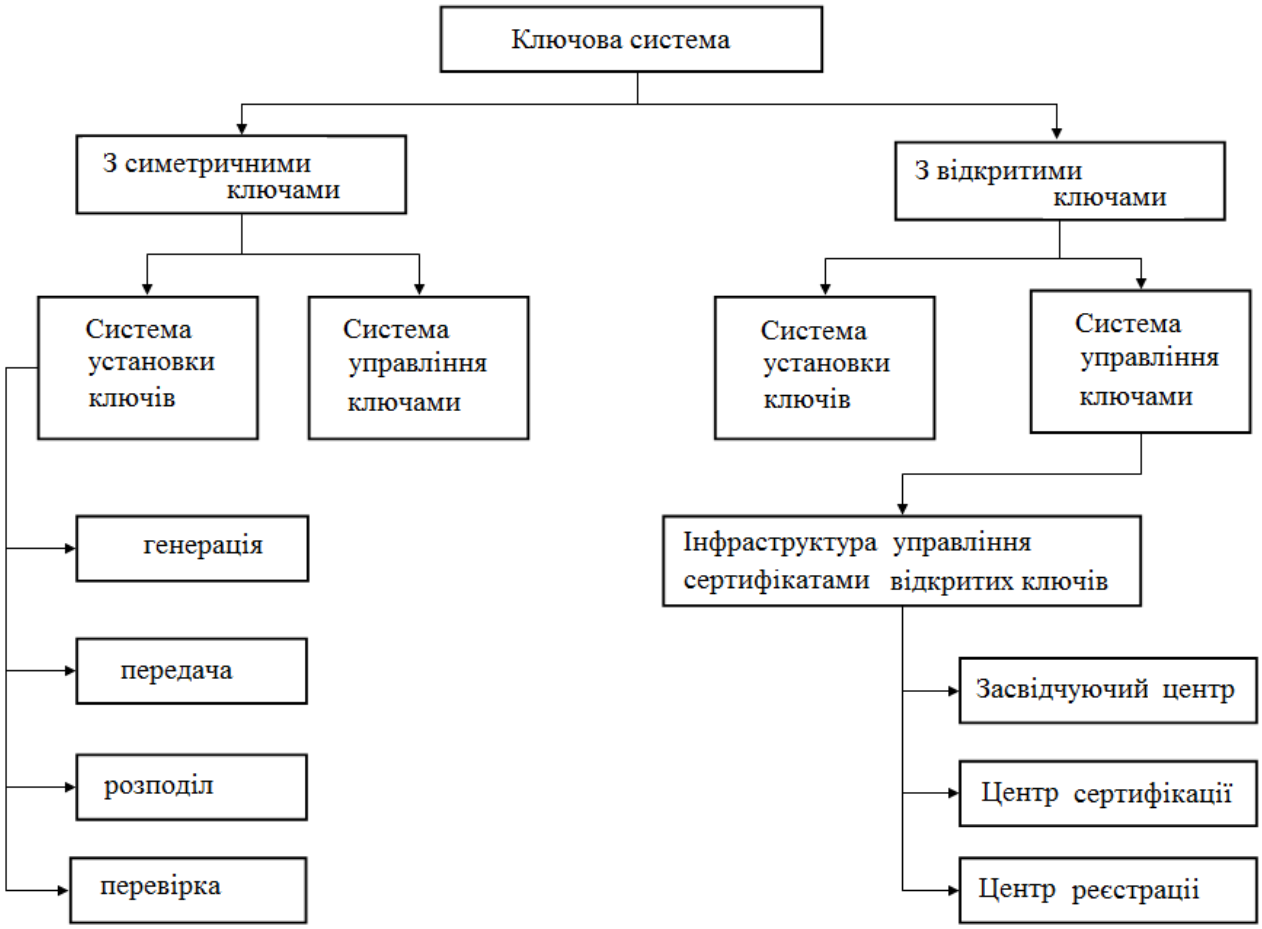

Рис. 1.3. Структура системи ключової

Система ключова асиметричною криптосистеми – заснована на використанні асиметричних ключів, що складаються з пари – відкритого і секретного (закритого) ключів. Основними проблемами таких систем є побудова системи управління ключами, яка, як правило, представляє собою інфраструктуру управління сертифікатами відкритих ключів, що включає центри реєстрації та сертифікації. Функції обох центрів можуть об'єднуватися в одному засвідчувальному центрі.

Стійкість криптографічна – властивість криптографічної системи, що характеризує її здатність протистояти атакам супротивника, як правило, з метою отримати ключ, відкрите повідомлення або нав'язати неправдиве повідомлення

1.2. ЕЛЕМЕНТИ КРИПТОСИСТЕМ

Алгоритм імітозащіщающего кодування інформації – алгоритм перетворення інформації (як правило, заснований на внесенні та використанні

надмірності) з метою контролю цілісності. На відміну від алгоритму формування цифрового підпису, використовує симетричні криптографічні системи. В якості такого перетворення може виступати код аутентифікації, автоматне і інші перетворення, або алгоритм шифрування.

Алгоритм перевірки цифрового підпису – алгоритм, в якості вихідних даних якого використовують підписане повідомлення, ключ перевірки і параметри схеми цифрового підпису, а результатом є висновок про правильність або помилковість цифрового підпису.

Алгоритм розшифрування – алгоритм, який реалізує функцію розшифрування.

Алгоритм формування цифрового підпису – алгоритм, в якості вихідних даних якого використовуються повідомлення, ключ підпису і параметри схеми цифрового підпису, а в результаті формується цифровий підпис.

Алгоритм шифрування – алгоритм, який реалізує функцію шифрування.

Життєвий цикл ключей – послідовність стадій, які проходять ключі від моменту генерації до знищення. Включає такі стадії, як: генерація ключів, реєстрація користувачів і ключів, ініціалізація ключів, період дії, зберігання ключа, заміна ключа, архівування, знищення ключів, відновлення ключів, скасування ключів.

Імітовставка – перевірочна комбінація, що додається до повідомлення для перевірки цілісності.

Імітостойкость – здатність протистояти активним атакам з боку противника, метою яких є нав'язування помилкового або підміна переданого повідомлення або збережених даних.

Код аутентифікації – алгоритм імітозахищаємого кодування інформації (як правило, обчислює значення імітовставки). До кодів аутентифікації пред'являються наступні вимоги: велика складність обчислення значення коду аутентифікації для заданого повідомлення без знання ключа; велика складність підбору для заданого повідомлення з відомим значенням коду аутентифікації іншого повідомлення з відомим значенням коду аутентифікації без знання ключа. Без знання секретного ключа ймовірність успішного нав'язування противником спотвореної або неправдивої інформації мала.

Відкриттй розподіл ключів (узгодження ключа, вироблення загального значення ключа) – протокол, що дозволяє двом абонентам виробити загальний секретний ключ шляхом обміну повідомленнями по відкритому каналу зв'язку без передачі будь-якої спільної секретної інформації, що розподіляється заздалегідь. Важливою перевагою відкритого розподілу є те, що жоден з абонентів заздалегідь не може визначити значення ключа, так як ключ залежить від повідомлень, переданих в процесі обміну.

Перешкодостійкість – здатність зберігати стійку роботу при наявності перешкод в каналі зв'язку.

Протокол – розподілений алгоритм, в якому беруть участь дві або більше сторони, що обмінюються між собою повідомленнями.

Протокол ідентифікації – протокол аутентіфікації сторін, що беруть участь у взаємодії і не довіряють один одному. Розрізняють протоколи односторонньою і взаємної ідентифікації. Протоколи ідентифікації, як правило, засновані на відомій обом сторонам інформації (паролі, особисті ідентифікаційні номери (PIN), ключі). На додаток до протоколу ідентифікації можуть використовуватися деякі фізичні прилади, за допомогою яких і проводиться ідентифікація (магнітна або інтелектуальна пластикова карта, або прилад, що генерує мінливі з часом паролі), а також фізичні параметри, складові невід'ємну приналежність доводить (підписи, відбитки пальців, характеристики голосу, геометрія руки та т. д.).

Протокол криптографічний – протокол, призначений для виконання функцій криптографічного системи, в процесі виконання якого сторони використовують криптографічні алгоритми.

Структура криптосистеми идентифікації представлена на рис. 1.4.

Протокол розподілу ключів – протокол, в результаті виконання якого взаємодіючі сторони (учасники, групи учасників) отримують ключі, які необхідні для функціонування криптографічного системи. Розрізняють такі типи протоколів розподілу ключів: протоколи передачі (вже згенерованих ключів); протоколи спільного вироблення загального ключа (відкритий

розподіл ключів) та схеми попереднього розподілу ключів. Залежно від порядку взаємодії сторін виділяють двосторонні протоколи, в яких сторони здійснюють передачу ключів при безпосередній взаємодії, або, інакше, протоколи типу «точка-точка», і протоколи з централізованим розподілом ключей, що передбачають наявність третьої сторони, яка грає роль довіреного центру.

Схема цифрового підпису складається з двох алгоритмів, один – для формування, а другий - для перевірки підпису. Надійність схеми цифрового підпису визначається складністю наступних трьох завдань для особи, яка не є власником секретного ключа: підробки підпису, тобто обчислення значення підпису під заданим документом; створення підписаного повідомлення, тобто знаходження хоча б одного повідомлення з правильним значенням підпису; підміни повідомлення, тобто підбору двох різних повідомлень з однаковими значеннями підпису.

Схема попереднього розподілу ключів складається з двох алгоритмів: розподілу вихідної ключової інформації і формування ключа. За допомогою першого алгоритму здійснюється генерація вихідної ключової інформації. Ця інформація включає відкриту частину, яка буде передана всім сторонам або поміщена на загальнодоступному сервері, а також секретні частини кожної сторони. Другий алгоритм призначений для обчислення діючого значення ключа для взаємодії між абонентами за наявною у них секретної та загальної відкритої частини вихідної ключової інформації. Він застосовується для зменшення обсягу збереженої і розподіленої секретної ключової інформації. Схема попереднього розподілу ключів повинна бути стійкою, тобто враховувати можливість розкриття частини ключів при компрометації, обмані або змові абонентів, і гнучкою: допускати можливість швидкого відновлення шляхом виключення скомпрометованих і підключення нових абонентів.

Функція криптографічна – функція, необхідна для реалізації криптографічного системи, наприклад, генерація ключів та псевдовипадкових послідовностей, оборотне перетворення, односпрямована функція, обчислення і перевірка значень імітовставки і цифрового підпису, обчислення значення хеш-

функції і т. п. Ці функції мають певні криптографічні властивости, впливають на криптографічну стійкість: залежність від ключа, складність звернення та ін.

Функція розшифрування здійснює перетворення безліч відкритих повідомлень в безліч зашифрованих повідомлень, залежних від ключа, є зворотним до перетворення, що здійснюється функцією шифрування [3].

Функція шифрування здійснює перетворення безліч відкритих повідомлень в безліч зашифрованих повідомлень, залежних від ключа.

Цифровий підпис (повідомлення або електронний документ) являє собою кінцеву цифрову послідовність, що залежить від самого повідомлення або документа і від секретного ключа, відомого тільки суб'єкту, який підписує, та призначена для встановлення авторства. Передбачається, що цифровий підпис має бути легко перевіряється без отримання доступу до секретного ключа. При виникненні спірної ситуації, пов'язаної з відмовою того, кто підписує від факту підпису деякого повідомлення або зі спробою підробки підпису, третя сторона повинна мати можливість вирішити суперечку. Цифровий підпис дозволяє вирішити наступні три завдання:

- здійснити аутентифікацію джерела даних;
- встановити цілісність повідомлення або електронного документа;
- забезпечити неможливість відмови від факту підпису конкретного повідомлення.

Структура криптосистеми цифрового підпису зображена на рис. 1.5.

Шифр – сімейство оборотних перетворень безлічі відкритих повідомлень в безліч зашифрованих повідомлень і назад, кожне з яких визначається деяким параметром, званим ключем. Математична модель шифру містить дві функції: шифрування та розшифрування, і модель безлічі відкритих повідомлень. Залежно від способу представлення відкритих повідомлень розрізняють блокові, потокові та інші шифри. Основними вимогами, що визначають якість шифру, є: криптографічна стійкість та імітостойкость.

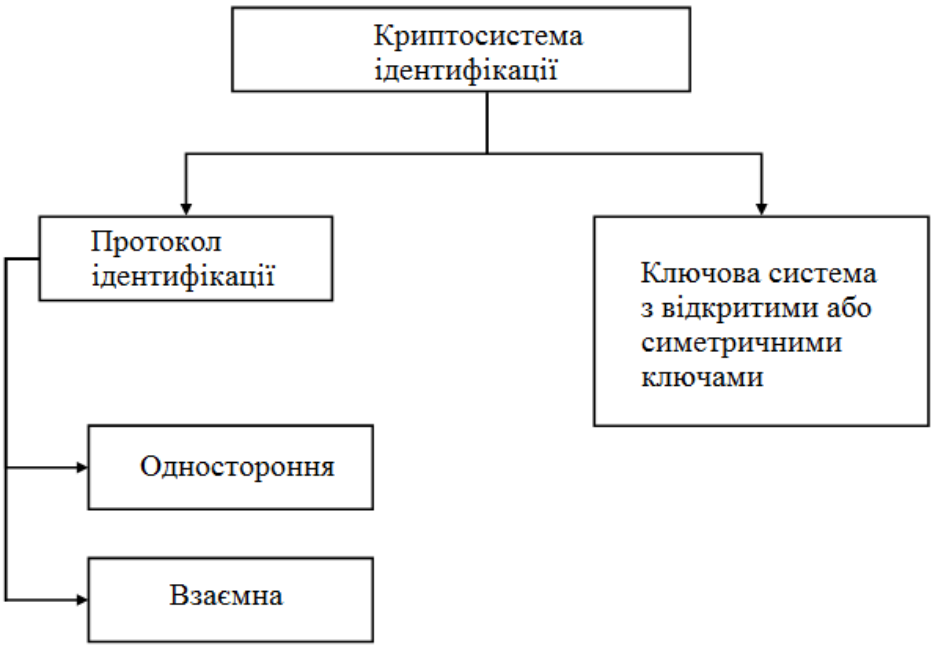

Рис. 1.4. Структура криптосистеми идентифікації

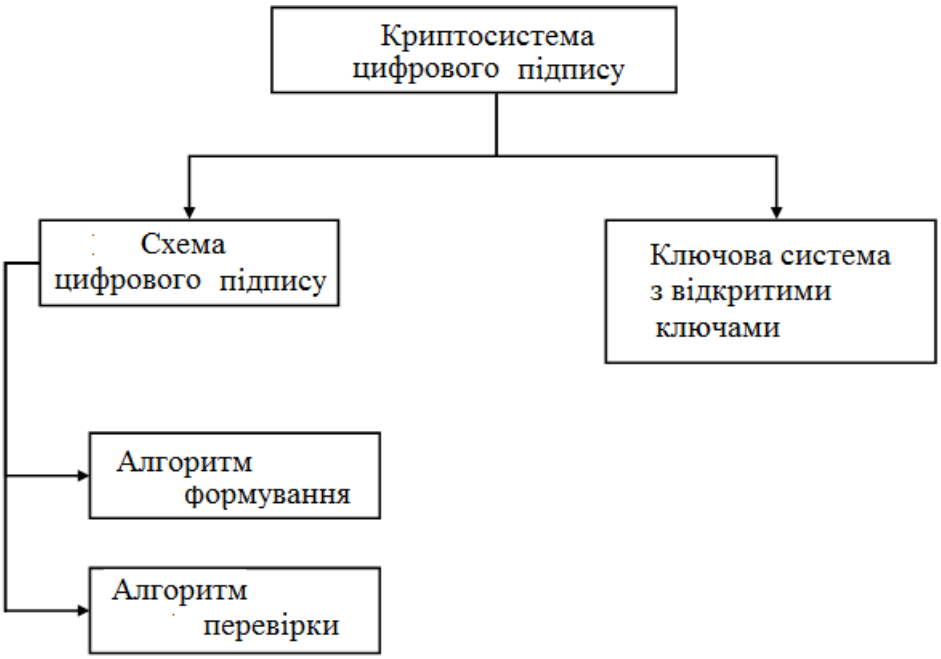

Рис. 1.5. Структура криптосистеми цифрового підпису

2. КРИПТОГРАФІЧНІ ПРОТОКОЛИ

2.1. ВИЗНАЧЕННЯ ПРОТОКОЛІВ

Існує кілька визначень криптографічних протоколів, але кожне з них посилається на визначення протоколу.

Протокол – це послідовність кроків, які роблять дві або більша кількість сторін для спільного вирішення деякої задачі. Всі кроки протоколу робляться в порядку суворої черговості, і жоден з них не може бути зроблений раніше, ніж закінчиться попередній. Згідно [1] протокол - це розподілений алгоритм вирішення деякої сукупності об'єктів і суб'єктів будь-якого завдання, кожен з яких досягає мети (вирішує завдання) з використанням приватних (розподілених) алгоритмів, причому при виконанні розподілених алгоритмів всі об'єкти і суб'єкти використовують однакову специфікацію даних і дій , процедури синхронізації і відновлення роботи після збоїв і ін.

Найпростіше визначення криптографічного протоколу дано в [3; 5] Криптографічний протокол – це протокол, який використовує криптографію. В [6], криптографічним протоколом називається протокол, в основі якого лежить криптографічний алгоритм.

Найбільш розгорнуте визначення криптографічного протоколу дано в [3]. Криптографічний протокол – протокол, призначений для виконання функцій криптографічного системи, в процесі виконання якого учасники використовують криптографічні алгоритми. Криптографічний система – це система, що забезпечує безпеку інформації криптографічними методами. Основними функціями криптографічної системи є забезпечення конфіденційності, цілісності, аутентифікації, неможливості відмови і включає підсистеми шифрування, ідентифікації, імітозахисту, цифрового підпису та ін., А також ключову систему.

Криптографічні протоколи повинні мати наступні властивості:

- Кожен учасник протоколу повинен знати протокол і всі необхідні кроки наперед;
- Кожен учасник повинен бути згоден йому слідувати;

- Протокол повинен бути чітко і однозначно визначено;
- Протокол повинен описувати реакцію учасників на будь-які ситуації, які можуть виникнути в ході його реалізації;
- Протокол повинен, бути повним, тобто приводити до вирішення поставленого завдання.

Типовий протокол передбачає від двох до чотирьох учасників. Один з них, наприклад, *A*, є ініціатором запуску протоколу. На підставі інформації, наявної у нього, він генерує інформацію для передачі, виконує над нею деяку послідовність дій, формує повідомлення і передає його учаснику *B* або *C* в залежності від даного протоколу. Користувач *B* (або *C*), отримавши повідомлення від *A*, виконує над ним відповідну послідовність дій, реєструє в своїй пам'яті виділену інформацію. На цьому завершується 1-ий цикл протоколу, а роль ініціатора передається учаснику *B* (або *C*).

Аналогічно, користувач В на підставі інформації, наявної тепер в його пам'яті, генерує інформацію для передачі, формує повідомлення і передає його *A* чи *C* в залежності від даного протоколу. Після прийому повідомлення, його обробки та реєстрації виділеної інформації в пам'яті одержувача завершується 2-ий цикл протоколу, і т.д.

Кожен учасник по протоколу має свою мету, що виражається в отриманні певної інформації.

Протокол завершується, коли кожен з учасників досягає своєї мети. В іншому випадку протокол обривається.

Крім учасників протоколу, які чесно його виконують, в протоколі можуть брати участь учасники-порушники (противники). Вони можуть бути активними і пасивними.

Пасивний супротивник тільки перехоплює всі повідомлення в каналі зв'язку, намагаючись витягти з них максимум інформації, але не втручаючись в протокол. Такий противник є неявним учасником протоколу, стан якого також має враховуватися і аналізуватися з точки зору безпеки протоколу.

Якщо ж противник активний, то він також стає несанкціонованим учасником протоколу, прихованим для санкціонованих учасників. Такий

противник не зобов'язаний дотримуватися протоколу. Він повинен тільки підтримувати видимість нормального виконання протоколу. Активний противник в протоколі може попеременно грати роль чесних (зареєстрованих) учасників протоколу. Він може підставляти замість повідомлень, переданих санкціонованими учасниками, повідомлення, передані в попередніх запусках протоколу, в поточному запуску, або, він може ініціювати від імені чесних учасників протоколу новий запуск протоколу до закінчення поточного і скористатися повідомленнями цього паралельного протоколу.

Ще більш сильним противником є такий, який володіє ключем (ключами), чинним або виведеним з дії, причому учасники протоколу про це можуть не знати, принаймні, в протягом деякого часу.

Розрізняють примітивні і прикладні криптографічні протоколи.

Примітивний криптографічний протокол – це криптографічний протокол, який не має самостійного прикладного значення, але використовується як базовий компонент при побудові прикладних криптографічних протоколів. Як правило, він вирішує будь-яку одну абстрактну задачу. Приклади: протокол обміну секретами, протокол прив'язки до біту, протокол підкидання монети (по телефону).

Прикладний криптографічний протокол призначений для вирішення практичних завдань забезпечення функцій - сервісів безпеки за допомогою криптографічних систем. Прикладні протоколи, як правило, забезпечують не одну, а відразу кілька функцій безпеки. Більш того, такі протоколи насправді є великими сімействами різних протоколів, що включають багато різних варіантів для різних ситуацій і умов застосування. Прикладами прикладних протоколів є: система електронного обміну даними, протоколи електронного документообігу; система електронних платежів, протокол підписання контракту, протокол сертифікованої електронної пошти та багато інших.

Щоб опис протоколів було більш наочним, їх учасники носять імена, які однозначно визначають ролі, їм уготовані. Розрізняють:

- протоколи з арбітражем (адвокатом);
- протокол із суддівством;

- самоствердджувальні протоколи.

Самоствердджувальні протоколи не вимагають присутності арбітра для завершення кожного кроку протоколу або наявності судді для вирішення конфліктних ситуацій. Самоствердджуються протокол влаштований так, що якщо один з його учасників шахраювати, інші зможуть моментально розпізнати нечесність, виявлену цим учасником, і припинити виконання наступних кроків протоколу.

У протоколах з арбітром, він є незацікавленим учасником протоколу, якому інші учасники повністю довіряють, роблячи відповідні дії для завершення чергового кроку протоколу. Учасники протоколу також беруть на віру все, що скаже арбітр, і беззаперечно виконують всім його рекомендаціям.

В силу того, що всі учасники протоколу повинні користуватися послугами одного й того ж арбітра, дії зловмисника, який вирішить завдати їм шкоди, будуть спрямовані, в першу чергу, проти цього арбітра. Отже, арбітр є слабкою ланкою в ланцюгу учасників будь-якого протоколу з арбітражем і тому протокол, в якому бере участь арбітр, часто ділиться на дві частини.

Перша повністю збігається зі звичайним протоколом без арбітражу, а до другої вдаються лише в разі виникнення розбіжностей між учасниками. Для вирішення конфліктів між ними використовується особливий тип арбітра – суддя. Подібно арбітру, суддя є незацікавленим учасником протоколу, якому інші його учасники довіряють при прийнятті рішень. Однак на відміну від арбітра, суддя бере участь аж ніяк не в кожному кроці протоколу. Послугами судді користуються, тільки якщо потрібно дозволити сумніви щодо правильності дій учасників протоколу. Якщо таких сумнівів ні у кого не виникає, суддівство не знадобиться. У комп'ютерних протоколах із суддівством передбачається наявність даних, перевіривши які довірена третя особа може вирішити, чи не зшахраював хто-небудь з учасників цього протоколу. Хороший протокол із суддівством також дозволяє з'ясувати, хто саме веде себе нечесно. Це служить прекрасним превентивним засобом проти шахрайства з боку учасників такого протоколу.

2.2. КЛАСИФІКАЦІЯ ПРОТОКОЛІВ

Зусиллями криптологів в різний час було створено велику кількість прикладних криптографічних протоколів [1; 3], які умовно можуть бути класифіковані за такими ознаками:

1 Класифікація за кількістю учасників: двосторонній, тристоронній і т. п.;

2 Класифікація за кількістю переданих повідомлень:

- інтерактивний (є взаємний обмін повідомленнями);
- неінтерактивний (тільки одноразова передача). Неінтерактивні протоколи часто називають схемами;

3 Класифікація за цільовим призначенням протоколу:

- протокол забезпечення цілісності повідомлень (з аутентифікацією джерела, без аутентифікації джерела);
- протокол (схема) цифрового підпису (протокол індивідуальної/групової цифрового підпису, з відновленням/без відновлення повідомлення, протокол цифрового підпису наосліп, протокол конфіденційної цифрового підпису, протокол цифрового підпису з доказовою підробки);
- протокол ідентифікації (аутентифікації) учасників (односторонньої аутентифікації, двосторонньої (взаємної) аутентифікації);
- протокол конфіденційної передачі (звичайний обмін повідомленнями, широкомовна/циркулярна передача, чесний обмін секретами, забуває передача;
- протокол розподілу ключів (схема попереднього розподілу ключів, передачі ключа (обміну ключами), спільного вироблення ключа (відкритого розподілу ключів), протокол парний/груповий, протокол (схема) поділу секрету, протокол (розподілу ключів для) телеконференції, і ін);

Класифікацію криптографічних протоколів можна проводити також і по іншим ознаками:

1 За типом використовуваних криптографічних систем:

- на основі симетричних криптосистем;

- на основі асиметричних криптосистем;
- змішані.

2 За способом функціонування:

- нтерактивний/неінтерактивний;
- однопрохідний/дво-/три- і т.д. прохідний;
- рротокол з арбітром (протокол з посередником),
- двосторонній/с довіреною третьою стороною (з центром довіри), і т.п.
- за складом і розподілу ролей;
- протоколи з арбітражем (адвокатом);
- протокол із суддівством;
- самоствердjуються протокол.

Будь-який криптографічний протокол після вдалого злому перестає бути надійним. Такі ситуації називають провалами протоколів. Існують приклади протоколів [2], які можуть бути абсолютно ненадійними і без всякого злому. Наприклад, протоколи, що розсилають ключі не за призначенням, протоколи з цифровим підписом, що легко підробити і т.д. Тому протоколи класифікують ще й за надійністю:

- імовірність злому протоколу не залежить від обсягу ресурсів і часу у зломщика;
- для зламу протоколу зловмисникові необхідно вирішити деяку математичну задачу, теоретично вирішувану, але для якої всі відомі на сьогодні у день методи вирішення потребують нездійсненно великого обсягу обчислень. Більшість відомих криптографічний протоколів належать до цього класу.

Здійснення зламу протоколу рівносильно, за обсягом необхідних зусиль і витрат, вирішенню якогось математично складного завдання (наприклад, підрахунок факторіала великого цілого).

- всі інші

2.3. ОПИС ПРОТОКОЛІВ

У сучасній літературі з криптографії найчастіше протоколи описуються в вербальному вигляді, що супроводжується пояснювальними діаграмами і/або символьним описом дій, які виконуються на кожному кроці протоколу і уточнююче специфікацію протоколу.

Загальновизнаного виду інтерфейсу протоколу не існує. Нижче наведені найбільш часто використовувані опису криптографічних протоколів:

1. Вербальний опис.

   Наприклад:

   1.2. Аліса і Боб вибирають систему шифрування.

   1.3. Аліса і Боб вибирають ключ.

   1.4. Аліса шифрує відкритий текст свого повідомлення з використанням алгоритму шифрування і ключа, отримуючи зашифроване повідомлення.

   1.5. Аліса посилає зашифроване повідомлення Бобу.

   1.6. Боб дешифрує шифротекст повідомлення з використанням алгоритму дешифрування і ключа, отримуючи відкритий текст повідомлення.

2. Математичний опис виконуваних операцій з вербальним описом дій учасників. Наприклад:

   Обчислюється значення хеш-функції від повідомлення *h (w)*.

   Далі учасник, що підписує, вибирає випадкове або псевдовипадкове значення *k*, *0 <k <q*, обчислює *k-1 (mod q)*, і генерує пару значень:

   r = gk (mod p) (mod q);

   s = к-1 (h (m) + xr) (mod q).

   Ця пара значень *(r, s)* і є електронним підписом під повідомленням *M*. Після створення цифрового підпису значення k знищується.

3. Описом по кроках протоколу. Приклад опису в таблиці 2.1.

Таблиця 2.1 - Протокол конфіденційного обміну

Цикл	Крок	Опис кроку
1	1	*A* формує текстову послідовність *M1*.
	2	*A* обчислює $S1 = E_{kAB}(M1)$.
	3	*A* відправляє учаснику *B* повідомлення *S1*.
	4	*B* отримує повідомлення *S1* і із заголовку дізнається ідентифікатор відправника *A*.
	5	*B* обчислює текст $M1 = D_{kAB}(S1)$.
2	1	*B* формує текстову послідовність *M2*.
	2	*B* обчислює $S2 = E_{kBA}(M2)$.
	3	*B* відправляє учаснику *A* повідомлення *S2*.
	4	*A* отримує повідомлення *S2, S1* і із заголовку дізнається ідентифікатор відправника *B*.
	5	*A* обчислює текст M2 $= D_{kBA}(S2)$.

4. Символічний опис. Приклад на рисунку 2.1.

$$A \rightarrow B : E_{kAB}(M_1)$$
$$A \leftarrow B : E_{kBA}(M_2)$$

Рисунок 2.1 – Приклад символічного опису протоколу

5. У вигляді відображення послідовності дій. Приклад на рисунку 2.2.

2.4. ВЛАСТИВОСТІ, ЩО ВИЗНАЧАЮТЬ БЕЗПЕКУ ПРОТОКОЛІВ

Оскільки криптографічний система може забезпечувати різні функції безпеки, для реалізації яких застосовують різноманітні криптографічні протоколи, то і властивостей, які характеризують безпеку криптографічного протоколу, також досить багато. Зазвичай властивості протоколів, що характеризують їх стійкість до різних атак, формулюють як цілі (goals) або

вимоги до протоколів. Трактування цих цілей з часом змінюється і уточнюється. Найбільш повне і сучасне тлумачення цих цілей дається в документах міжнародної організації Internet Engineering Task Force (IETF).

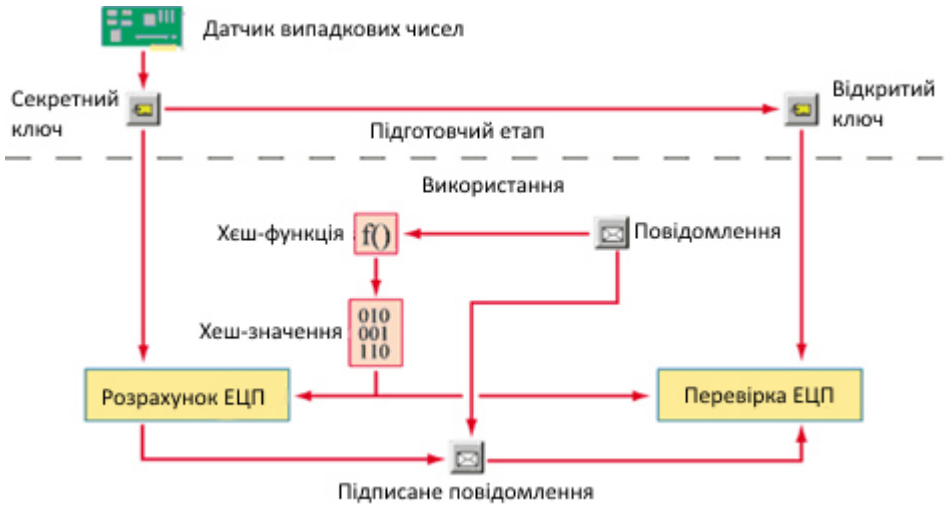

Рисунок 2.2 – Ілюстрація «Відображення послідовності дій»

У документах IETF фігурують двадцять властивостей (цілей, вимог) безпеки, розподілених по десяти групам (див таб.2.2). Наведемо ці властивості.

Аутентифікація (не широкомовна) – перевірка ідентичності, заявленої учасником або суб'єктом системи, в якості якого може виступати одна зі сторін комунікації або джерело деяких даних. Аутентифікація зазвичай є односторонньою. Взаємна аутентифікація здійснюється в обох напрямках.

G1 – аутентифікація суб'єкта (аутентифікація сторін. Це перевірка з підтвердженням справжності однієї зі сторін або наявності повноважень (за допомогою наданих доказів і (або) документів) ідентичності другої сторони, що бере участь у виконанні протоколу, а також того, що вона дійсно бере участь у виконанні протоколу.Зазвичай така перевірка здійснюється за допомогою набору даних, який міг бути згенерований тільки вторим учасником (наприклад, відгук на запит). Таким чином, зазвичай аутентифікація суб'єкта має на увазі, що деякі дані можуть бути безпомилково повернуті деякого суб'єкту, що передбачає аутентифікацією джерела даних (англ. *data origin authentication*).

Таблиця 1.2 – Групи властивостей безпеки криптографічних протоколів

Група безпеки	Властивість (ціль, вимоги)
Аутентифікація(не широкомовна)	G1 – аутентифікація суб'єкта
	G2 – аутентифікація повідомлення
	G3 – захист від повтору
Аутентифікація при розсилці за багатьма адресами або встановлення з'єднання зі службою підписки / повідомлення	G4 – неявна (прихована) аутентифікація одержувача
	G5 – аутентифікація джерела
Авторизація (довіреною третьою стороною)	G6 – авторизація (довіреною третьою стороною)
Властивості спільної генерації ключа	G7 – аутентифікація ключа
	G8 – підтвердження вірності ключа
	G9 – захищеність від читання назад
	G10 – формування нових ключів
	G11 – захищена можливість домовитися про параметри безпеки
Конфіденційність	G12 – конфіденційність
Анонімність	G13 – захист ідентифікаторів від прослуховування
	G14 – захист ідентифікаторів від інших учасників
Захищеність від атак типу «відмова в обслуговуванні»	G15 – обмежена захищеність від атак типу «відмова в обслуговуванні»
Інваріантність відправника	G16 – інваріантність відправника
Неможливість відмови від раніше вчинених дій	G17 – підзвітність
	G18 – доказ джерела
	G19 – доказ одержувача
Безпечна тимчасова властивість	G20 – безпечна тимчасова властивість

***G2* – аутентифікація повідомлення**. Полягає в забезпеченні аутентифікації джерела даних і цілісності переданого повідомлення. Аутентифікація джерела даних означає, що протокол повинен забезпечувати засоби гарантії того, що отримане повідомлення або частина даних були створені деякими учасником в певний момент часу, що передує одержанню повідомлення, і що ці дані не були спотворені або підроблені, але без надання гарантій однозначності і своєчасності.

***G3* – захист від повтору**. Це гарантування одним з учасників того, що аутентифіковане повідомлення не є старим (було згенеровано в даному сеансі протоколу, або протягом відомого проміжку часу, або повідомлення не було прийнято раніше.Аутентифікація при розсилці за багатьма адресами або встановлення з'єднання зі службою підписки / повідомлення – це вимога аутентифікації для груп учасників з одним джерелом і великим числом потенційних одержувачів (широкомовна передача) або джерело і служба, які відправляють інформацію підключеним і авторизованим користувачам.

***G4* – неявна (прихована) аутентифікація одержувача**. Протокол повинен надавати кошти гарантії того, що відправлене повідомлення буде прочитано тільки тими сторонами, яким воно було адресоване, тобто тільки законні авторизовані учасники отримають доступ до поточної інформації, широкомовним повідомленням або групової комунікації (передачі);

***G5* – аутентифікація джерела**. Законні групи учасників повинні бути здатні аутентифікувати джерело і зміст інформації або групової комунікації. Це стосується випадків, коли групи учасників не довіряють один одному.

Авторизація довіреною третьою стороною.

G6 – полягає в тому, що в деяких протоколах довірена третя сторона представляє одного суб'єкта В іншому суб'єкту *A*. В результаті цього суб'єкт *A* отримує гарантії того, що суб'єкт *B* посвідчений за допомогою довіреної третьої сторони і авторизований (наділений правами) в необхідному для протоколу сенсі . Коли протокол виконується трьома учасниками *A*, *B*, довірена третя сторона, то суб'єкт *A*, ймовірно, не може мати доступ до контрольного списку

або іншим механізмам для авторизації *B* (бо ім'я *B* невідомо суб'єкту *A* або може бути псевдонім), але суб'єкт *A* отримує гарантії того, що суб'єкт *B* авторизований довіреною третьою стороною.

Властивості спільної генерації ключа.

***G7* – аутентифікація ключа**. Це властивість передбачає, що один з учасників отримує підтвердження того, що ніякий інший учасник крім заздалегідь визначеного другого учасника (і, можливо, інших довірених учасників) не може отримати доступ до жодного секретного ключа;

***G8* – підтвердження вірності ключа**. Один з учасників отримує підтвердження того, що другий учасник (можливо, невизначений) дійсно володіє конкретним секретним ключем (або має доступ до всіх ключових матеріалів, необхідних для його обчислення);

***G9* – захищеність від читання назад** / досконала таємність в майбутньому. Протокол володіє цією властивістю, якщо компрометація довгострокових ключів не призводить до компрометації старих сеансових ключів;

***G10* – формування нових ключів**. Протокол використовує динамічний розподіл ключів з метою отримання нових ключів;

***G11* – захищена можливість домовитися про параметри безпеки**. Якщо протокол відкритого розподілу ключів дає можливість сторонам домовлятися про параметри безпеки (таких як ідентифікатори захищеної асоціації, довжина ключа і набори алгоритмів шифрування), то ця властивість важлива для підтвердження того, що заявлені властивості і параметри, про які домовилися учасники протоколів, не були підмінені зловмисником.

Конфіденційність

G12 – конфіденційність полягає в тому, що специфічний набір даних (зазвичай посилається або отримується як частина «захищеного» повідомлення, а також сформований на основі даних, отриманих в результаті обміну) не стане доступним або розкритим для неавторизованих суб'єктів або процесів, а залишиться невідомим противнику. Секретність сеансового ключа, згенерованого в результаті процедури відкритого розподілу ключів,

розглядається при описі властивості G7. Секретність довготривалого ключа, використовуваного в протоколі, не розглядається як цільове властивість безпеки протоколу, а відноситься до вихідних припущеннями.

Анонімність. Багато протоколів не забезпечують властивості анонімності, оскільки, як правило, сторона хоче знати, з ким вона взаємодіє при формуванні ключа. Однак деякі протоколи дозволяють приховувати ідентифікатори.

***G13* – захист ідентифікаторів від прослуховування**. Атакуючий, який здійснює перехоплення повідомлень; не повинен мати можливість зв'язати повідомлення одного з учасників з самим учасником;

***G14* – захист ідентифікаторів від інших учасників**. В процесі взаємодії інші учасники не повинні мати можливості зв'язати повідомлення конкретного учасника з самим учасником, а тільки з непов'язаним з ним псевдонімом або приватним ідентифікатором.

Обмежена захищеність від атак типу "Відмова в обслуговуванні".

***G15* – обмежена захищеність** від атак типу "відмова в обслуговуванні" полягає в тому, що важко забезпечити захищеність від *DoS*-атак. Протокол може бути об'єктом *DoS*-атак з різних причин; найпоширеніша полягає в тому, що протокол споживає занадто багато ресурсів (пам'яті, обчислювальної потужності), перед тим як сторони аутентифікують один одного.

Інваріантність відправника.

***G16* – інваріантність відправника** полягає в тому, що учасник отримує гарантії того, що джерело повідомлень не змінювалось з початку виконання сеансу, хоча саме встановлення ідентичності цього джерела для одержувача не важливо.

Неможливість відмови від раніше вчинених дій передбачає запобігання того, що учасник відмовиться від реально вчиненого ним дії.

G17 – підзвітність. Ця властивість системи, складається у тому, що надаються гарантії того, що дії системних суб'єктів можуть бути однозначно простежено тими суб'єктами, хто відповідає за ці дії;

***G18* – доказ джерела**. Це безперечний доказ (очевидність) того, що повідомлення було відправлено;

***G19* – доказ отримання**. Це безперечний доказ (очевидність) того, що повідомлення було отримано.

Безпечна тимчасова властивість.

G20 – безпечне тимчасове властивість полягає в тому, що використовуючи два оператора часової логіки (лінійної часової логіки), а саме оператора «завжди» і «колись в минулому», можна формалізувати властивості виду: «Для будь-якого досяжного стану, що має властивість p , раніше був стан з властивістю q».

У деяких документах *IETF* обговорюються нові властивості безпеки.

Формування сеансу. Протокол забезпечує формування сеансу, якщо він пов'язує кожен конкретний сеанс протоколів з унікальним значенням, узагальненим ідентифікатором сеансу, який зазвичай є набором випадкових даних і ідентифікаторів. Цей узагальнений ідентифікатор сеансу дозволяє відрізнити кожен конкретний сеанс протоколу від інших сеансів цього протоколу. Після виконання початкової частини протоколу всі повідомлення містять узагальнений ідентифікатор сеансу (не обов'язково у відкритому вигляді).

Послідовне уявлення. Після виконання будь-якої частини протоколу всі учасники даного сеансу протоколу мають однакове уявлення про всіх учасників цього сеансу і виконуваних ними ролях, а також про стан виконання протоколу.

Іменування ключів. Для того щоб мати гарантії від неправильного використання ключових матеріалів у кожній захищеній асоціації протоколу обміну, криптографічний протокол повинен використати наявні імена ключів і відповідний контекст, що дозволяє інформувати перевіряючого про порядок використання цього ключового матеріалу. Якщо протокол забезпечує доказ володіння ключами, то протокол повинен застосовувати явні імена ключів, що використовуються протягом докази володіння, щоб запобігти ситуації, коли використовується більше одного набору матеріалів для виконання протоколу обміну.

Є і інші властивості, обговорювані в документах *IETF*, наприклад: криптографічний поділ ключів, можливість домовитися про вибір алгоритмів шифрування, стійкість до атаки зі словником, криптографічне зв'язування, підтримка швидкого відновлення з'єднання, підтвердження успішного

завершення і повідомлень про помилку, незалежність сеансів, захищеність від атаки противник в середині і ін.

2.5 АТАКИ НА ПРОТОКОЛИ

Під атакою на протокол розуміється спроба проведення аналізу повідомлень протоколу і / або виконання не передбачених протоколом дій з метою порушення роботи протоколу і / або отримання інформації, що становить секрет його учасників. Атака вважається успішною, якщо порушено хоча б один з номінальних параметрів, що характеризують безпеку протоколу (див. табл. 2.2).

В основі атак можуть лежати різні методи аналізу протоколів.

Атаки на протоколи бувають спрямовані проти криптографічних алгоритмів, які в них задіяні, проти криптографічних методів, що застосовуються для їх реалізації, а також проти самих протоколів.

Ці атаки умовно можна розділити на наступні групи:

- Пасивні (підслуховування протоколу з метою отримання інформації);
- Активні (спроби змінити протокол – вставити, змінити повідомлення);
- Пасивні шахраї – одна зі сторін намагається отримати більше інформації, не перестаючи при цьому дотримуватися протоколу;
- Активні шахраї – одна зі сторін, намагається змінити протокол.

Особа, яка не є учасником протоколу, може спробувати підслухати інформацію, якою обмінюються його учасники. Це пасивна атака на протокол, яка названа так тому, що атакуючий може тільки накопичувати дані і спостерігати за ходом подій, але не в змозі впливати на нього.

Пасивна атака подібна крипто-аналітичній атаці зі знанням тільки шифротекста. Оскільки учасники протоколу не володіють надійними засобами, що дозволяють їм визначити, що вони стали об'єктом пасивної атаки, для захисту від неї використовуються протоколи, що дають можливість запобігати можливі несприятливі наслідки пасивної атаки, а не розпізнавати її.

Атакуючий може спробувати внести зміни до протоколу заради власної вигоди. Він може видати себе за учасника протоколу, внести зміни в повідомлення, якими обмінюються учасники протоколу, підмінити інформацію, яка зберігається в комп'ютері і використовується учасниками протоколу для прийняття рішень. Це активна атака на протокол, оскільки атакуючий може втручатися в процес виконання кроків протоколу його учасниками. Отже, пасивно атакуючий намагається зібрати максимум інформації про учасників протоколу і про їхні дії.

У активно атакуючого ж зовсім інші інтереси – погіршення продуктивності комп'ютерної мережі, отримання несанкціонованого доступу до її ресурсів, внесення спотворень в бази даних. При цьому всі атакуючі не обов'язково є абсолютно сторонніми особами. Серед них можуть бути легальні користувачі, системні і мережеві адміністратори, розробники програмного забезпечення і навіть учасники протоколу, які поводяться непорядно або навіть зовсім не дотримуються цей протокол. В останньому випадку атакуючий учасник протоколу називається шахраєм.

Пасивний шахрай слідує усім правилам, які визначені протоколом, але при цьому ще й намагається дізнатися про інших учасників більше, ніж передбачено цим протоколом.

Активний шахрай вносить довільні зміни в протокол, щоб нечесним шляхом добитися для себе найбільшої вигоди.

Захист протоколу від дій декількох активних шахраїв є вельми нетривіальною проблемою. Проте за деяких умов цю проблему вдається вирішити, надавши учасникам протоколу можливість вчасно розпізнати ознаки активного шахрайства. А захист від пасивного шахрайства повинен надавати будь-який протокол незалежно від умов, в які поставлені його учасники.

Найбільш широко відомі атаки на криптографічні протоколи:

- Підміна – спроба підмінити одного користувача іншим. Порушник, виступаючи від імені однієї зі сторін і повністю імітуючи її дії,

отримує у відповідь повідомлення певного формату, необхідні для підробки окремих кроків протоколу;

- Повторне нав'язування повідомлення – повторне використання раніше переданого в поточному або попередньому сеансі повідомлення або будь-якої його частини в поточному сеансі протоколу. Наприклад, повторна передача інформації раніше проведеного протоколу ідентифікації може привести до повторної успішної ідентифікації того ж самого або іншого користувача. У протоколах передачі ключів ця атака часто застосовується для повторного нав'язування вже використаного раніше сеансового ключа - атака на основі новизни;
- Атака відображенням. Цей тип атак пов'язаний зі зворотним передачею адресату раніше переданих їм повідомлень. Часто атаки даного типу відносять до класу атак з повторним нав'язуванням повідомлення;
- Затримка передачі повідомлення – перехоплення противником повідомлення і нав'язування його в більш пізній момент часу. Це різновид атаки з повторним нав'язуванням повідомлення;
- Комбінована атака – підміна або інший метод обману, який використовує комбінацію даних з раніше виконаних протоколів, в тому числі протоколів, раніше нав'язаних супротивником;
- Атака з паралельними сеансами. Спеціальний окремий випадок попередньої атаки, в якому противник спеціально відкриває одночасно кілька паралельних сеансів з метою використання повідомлень з одного сеансу в іншому;
- Атака з використанням спеціально підібраних текстів - атака на протоколи типу «запит - відповідь» при якій противник за певним правилом вибирає запити з метою отримати інформацію про довготривале ключі доводить. Ця атака може включати спеціально підібрані відкриті тексти, якщо доводить повинен підписати або

зашифрувати запит або шифровані тексти, якщо доводить повинен розшифрувати запит;

- Атака «противник в середині». Використовується противником своїх коштів в якості частини телекомунікаційної структури. Атака, при якій в протоколі ідентифікації між *A* і *B* противник входить в телекомунікаційний канал і стає його частиною при реалізації протоколу між *A* і *B*. При цьому противник може підмінити інформацію, передану між *A* і *B*. Ця атака особливо небезпечна в разі формування учасниками *A* і *B* загального ключа по протоколу Діффі – Хеллмана;
- Атака з відомим сеансовим ключем. У багатьох випадках проведення атаки полегшує додаткова інформація. Атака полягає у спробі отримання інформації про довготривалі ключі або будь-якої іншої ключової інформації, що дозволяє відновлювати сеансові ключі для інших сеансів протоколу;
- Атака з невідомим спільним ключем – атака, при якій порушник відкриває два сеанси з двома зареєстрованими учасниками, виступаючи в першому випадку від імені одного з них, хоча останній може нічого не знати про це. При цьому в результаті буде сформований загальний ключ між чесними учасниками, причому один з них буде впевнений, що сформував загальний ключ іншим чесним учасником;

Існує велика кількість і інших типів атак, які залежать від конкретної реалізації протоколу.

2.6 АНАЛІЗ І МОДЕЛЮВАННЯ ПРОТОКОЛІВ

З точки зору додатків аналіз протоколів має дуже велике значення, тому що саме за допомогою протоколів принципи криптографії знаходять практичне застосування. Самі алгоритми шифрування безумовно також значимі, але є лише частиною протоколу. І надійність алгоритму аж ніяк не забезпечує

безпеку протоколу, що його використовує. Криптографічний протокол забезпечує досягнення певних цілей безпеки. Однак, якщо протокол містить помилки, то він може не досягти або досягти не в повній мірі усіх поставлених перед ним цілей. Помилки в протоколі можуть бути неявними і важко виявляються. Існує безліч прикладів, коли помилки виявлялися в уже добре вивчених протоколах.

Багато системи «втрачають гарантію» безпеки, якщо використовуються неправильно. Так наприклад алгоритми шифрування необов'язково забезпечують цілісність даних, а протоколи обміну ключами необов'язково гарантують, що обидві сторони отримають той самий ключ. Ще одне можливе слабке місце - взаємодія між окремо безпечними протоколами шифрування [5].

Майже для кожного безпечного протоколу, як правило, можна знайти інший, не менш надійний, який зведе нанівець всі переваги першого, якщо вони обидва використовують однакові ключі на одному і тому ж пристрої.

Якщо різні стандарти захисту застосовуються в одному середовищі, недостатньо чітка взаємодія між ними часто може привести до небажаних наслідків. Багато цікавих способів подолання захисних рубежів пов'язані з моделями довірчих відносин всередині системи. Прості системи (засоби шифрування телефонних переговорів та інформації на жорстких дисках) використовують елементарні довірчі моделі. Комплексні системи (засоби електронної торгівлі або засоби захисту багатокористувацьких пакетів електронної пошти) побудовані на основі складних (і набагато більш надійних) моделей довірчих відносин, що описують взаємозв'язку безлічі елементів.

Аналіз протоколу зводиться до ретельної формальної перевірки всіх можливих ситуацій.

Нижче наведені три загальних правила, яким слідують при аналізі криптографічних протоколів [2]:

1 Для всіх величин, які використовуються в протоколі, слід перерахувати всі їх властивості - як явно зазначені в специфікації протоколу, так і неявно передбачувані;

2 Слід вивчати поведінку протоколу при всіх можливих відхиленнях неявно заданих властивостей параметрів. Треба розглядати поведінку протоколу при зміні не тільки окремих параметрів, але їх комбінацій;
3 Якщо з'ясується, що на хід протоколу можна вплинути зміною тих чи інших параметрів і тому слід з'ясувати наскільки серйозними будуть наслідки такої зміни.

Існує чотири основні підходи до аналізу криптографічних протоколів [1;3]:

1 Моделювання і перевірка роботи протоколу з використанням мов опису і засобів перевірки не розроблених спеціально для аналізу криптографічних протоколів;
2 Створення експертних систем, що дозволяють конструктору протоколу розробляти і досліджувати різні сценарії;
3 Вироблення вимог до сімейства протоколів, використовуючи якусь логіку для аналізу понять «знання» і «довіру»;
4 Розробка формальних методів, заснованих на записи властивостей криптографічних систем в алгебраїчному вигляді.

Перший з підходів намагається довести правильність протоколу, розглядаючи його як звичайну комп'ютерну програму. Ряд дослідників представляють протокол як кінцевий автомат, інші використовують розширення методів обчислення предиката першого порядку, а треті для аналізу протоколів використовують мови опису. Однак, доказ правильності аж ніяк не є доказом безпеки, і цей підхід зазнав невдачі при аналізі багатьох «дірявих» протоколів. І хоча його використання спочатку широко вивчалося, з ростом популярності третього і четвертого підходів, роботи в цій галузі були переорієнтовані.

У другому підході для визначення того, чи може протокол перейти в небажаний стан (наприклад, втрата ключа), використовуються експертні системи. Хоча цей підхід дає кращі результати при пошуку «дірок», він не гарантує безпеки і не надає методик розробки розтинів. Він хороший для перевірки того, чи містить протокол конкретну «діру», але навряд чи здатний виявити невідомі «дірки» в протоколі.

Третій підхід набагато популярніше. Він був вперше введений Майклом Берроуз, Мартіном Абеді і Роджером Неедхемом. Вони розробили формальну логічну модель для аналізу знання і довіри, названу БАН-логікою. БАН-логіка є найбільш широко розповсюдженою при аналізі протоколів перевірки автентичності. Вона розглядає справжність як функцію від цілісності і новизни, використовуючи логічні правила для відстеження стану цих атрибутів протягом усього протоколу. БАН-логіка не надає доказ безпеки, вона може тільки розмірковувати про перевірку достовірності. Вона є простою, прямолінійною логікою, легкою в застосуванні і корисною при пошуку «дірок» в протоколах.

Методи четвертого, формального підходу, з одного боку досить змістовні і дозволяють легко виконувати моделювання та аналіз протоколів; з іншого боку, вони досить складні і дозволяють виявляти складні для розуміння помилки, не виявлені при неформальному аналізі. Формальні методи протягом тривалого часу використовувалися для аналізу комунікаційних протоколів. Деякі роботи з аналізу криптографічних протоколів велися в кінці сімдесятих і на початку вісімдесятих років [6]. Але в цілому, застосування формальних методів до криптографічних протоколів не було широко поширене до початку дев'яностих, коли при використанні методів формального аналізу були знайдені невиявлені раніше помилки в криптографічних протоколах.

Більшість формальних методів, засновані на теорії кінцевих автоматах і використовують модель зловмисника, запропоновану Долевим і Яо [3; 5]. У моделі Долева-Яо всі активні учасники протоколу поділяються на два види: чесні учасники і зловмисник. Чесні учасники виконують кроки протоколу без відхилень. Вони можуть одночасно виконувати кілька сеансів протоколу з різними учасниками. Модель містить повідомлення, якими обмінюються учасники протоколу, але не описує внутрішні стану учасників. У моделі Долева і Яо робиться припущення, що середовище передачі контролюється зловмисником, який може читати весь трафік, змінювати і видаляти повідомлення, створювати нові повідомлення, і виконувати будь-які операції які можуть виконувати законні користувачі системи. Передбачається, що

спочатку зловмисник не знає ніякої секретної інформації, наприклад секретних ключів належать легітимним користувачам системи. Оскільки зловмисник може видаляти повідомлення з каналу зв'язку і поміщати в канал зв'язку створені ним повідомлення, то можна розглянути будь-яке повідомлення, надіслане легітимним користувачем, як повідомлення, надіслане зловмисникові, і будь-яке повідомлення, отримане легітимним користувачем, як повідомлення, отримане від зловмисника. Таким чином, система стає автоматом, використовуваним зловмисником для генерації слів. Ці слова підкоряються певним правилам підстановки, наприклад таким, що шифрування і розшифрування на одному ключі. Таким чином, зловмисник управляє системою з підстановкою елементів. Якщо мета зловмисника полягає в тому, щоб дізнатися секретне слово, то проблема докази безпеки протоколу стає проблемою визначення слова в системі з підстановкою елементів. Долев і Яо, використовуючи останній висновок, створили кілька алгоритмів для аналізу обмеженої множини протоколів. Модель Долева і Яо занадто обмежена і не підходить для аналізу багатьох протоколів. Вона може використовуватися тільки для виявлення помилок, які можуть призвести до порушення конфіденційності. Більшість методів аналізу протоколів, що використовують модель зловмисника Долева і Яо, розширюють її, щоб описати поведінку учасників протоколу.

КОНТРОЛЬНІ ПИТАННЯ

1. Що таке конфіденційність та аутентифікація?

2. Перерахуйте видомі Вам види криптосистем.

3. З яких алгоритмів складається схема попереднього розподілу ключів?

4. Дайте характеристику криптографічної функції та функціям розшифрування та шифрування.

5. Що таке протокол и які протоколи Вам відомі?

6. Що являє собою цифровий підпис?

7. Що таке шифр?

8. Дайте визначення поняття «криптографічний протокол».

9. Які властивості повинні мати криптографічні протоколи?

10. Що таке примітивні і прикладні криптографічні протоколи?

11. За якими ознаками умовно можуть бути класифіковані прикладні криптографічні протоколи?

12. Дайте характеристику групам безпеки криптографічних протоколів?

13. Що розуміється під атакою на протокол?

14. На які групи умовно можна розділити ці атаки?

ЛИТЕРАТУРА

1. Тилборг ван Х.К.А. Основы криптологии /Тилборг ван Х.К.А. – М.: Мир, 2006. – 471 с.

2. Защита информации в системах телекомуникации: Учебное пособие для вузов / [Банкет В.Л. и др.]. – Од., УГАС им. А.С. Попова, 1997. – 96 с.

3. Гулак Г. Різні підходи до визначення випадкових послідовностей: /Г.Гулак. Л.Ковальчук// Науково-технічний збірник «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні». – 2001. - №3 – С. 127-133.

4. Б. Шнайер Прикладная криптография. Теория и практика/ Венбо Мао; [пер. с англ.] . – М.: Изд.дом «Вильямс». 2005. – 786 с.

5. Бессалов А.В. Криптосистемы на эллиптических кривых / А.В. Бессалов, А.Б. Телиженко. – К.: ІВЦ Видавництво «Політехніка», 2004. – 224.

6. Вербицький О. Вступ до криптології/ Вербицький О. – Львів : Видавництво науково- технічної літератури, 1998. – 247 с.

Упорядники:

Саксонов Геннадій Михайлович

Жукова Олена Андріївна

КОНСПЕКТ ЛЕКЦІЙ

з дисципліни «Методи побудови та аналізу криптосистем»

для студентів-магістрів спеціальності 125 Кібербезпека
галузі знань 12 Інформаційні технології

Видано в редакції упорядників

Комп'ютерний дизайн, верстка та обробка – Г.М. Саксонов

Підписано до друку 25.04.2019. Формат 30х42/4.
Папір офсетний. Ризографія. Ум. друк. арк. 2,1.
Обл.-вид. арк. 2,1. Тираж 6 пр. Зам. №

Національний технічній університет «Дніпровська політехніка»

49005, м. Дніпро, просп. Д. Яворницького, 19