ОСОБЛИВОСТІ КРИПТОГРАФІЧНОГО ЗАХИСТУ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Сергій Гнатюк, Василь Кінзерявий, Андрій Охріменко

Національний авіаційний університет

ГНАТЮК Сергій Олександрович, к.т.н.

Рік та місце народження: 1985 рік, м. Нетішин, Хмельницька область, Україна.
Освіта: Національний авіаційний університет, 2007 рік.
Посада: доцент кафедри безпеки інформаційних технологій з 2012 року.
Наукові інтереси: інформаційна безпека, управління інцидентами інформаційної безпеки, квантова криптографія.
Публікації: більше 90 наукових публікацій, серед яких монографія, наукові статті у фахових вітчизняних та міжнародних виданнях, тези та матеріали доповідей на конференціях, патенти на винаходи та авторські свідоцтва.
E-mail: s.gnatyuk@nau.edu.ua

КІНЗЕРЯВИЙ Василь Миколайович

Рік та місце народження: 1985 рік, м. Кам'янець-Подільський, Хмельницька область, Україна.
Освіта: Національний авіаційний університет, 2007 рік.
Посада: асистент кафедри безпеки інформаційних технологій з 2009 року.
Наукові інтереси: криптографічний захист інформації, криптоаналіз симетричних шифрів.
Публікації: більше 40 наукових публікацій, серед яких наукові статті, тези та матеріали доповідей на конференціях, патенти на винаходи та авторські свідоцтва.
E-mail: 0werl0rd@ukr.net

ОХРІМЕНКО Андрій Олександрович

Рік та місце народження: 1990 рік, м. Васильків, Київська область, Україна.
Освіта: Національний авіаційний університет, 2012 рік.
Посада: магістрант кафедри безпеки інформаційних технологій.
Наукові інтереси: криптографія, аналіз та оцінка інформаційних ризиків.
Публікації: більше 30 наукових публікацій, серед яких наукові статті, тези доповідей та авторські свідоцтва.
E-mail: andrew.okhrimenko@gmail.com

Анотація. *У даній статті наведено базові принципи побудови абстрактної моделі порушника в державних інформаційно-комунікаційних системах. Розглядаються основні принципи побудови різного типу криптосистем, які можуть використовуватися для захисту державних інформаційних ресурсів. Крім того, проаналізовано основні проблеми управління ключовими даними в процесі захисту державних інформаційних ресурсів.*

Ключові слова: *державні інформаційні ресурси, абстрактна модель порушника, криптографія, генерація та розподіл ключів шифрування, принципи криптографії.*

Вступ

Сучасний світ характеризується тенденцією постійного підвищення ролі інформації, яка має усе більш вагоме значення у функціонуванні державних і суспільних інститутів, в житті кожної людини. У сучасних умовах сформувався новий вид трудової діяльності, пов'язаний із здобуттям, поширенням і зберіганням інформації. Промислове суспільство трансформується в інформаційне. Інформатизація веде до створення єдиного світового інформаційного простору, до уніфікації інформаційних технологій різних країн. Нові технології обіцяють грандіозні перспективи. У той же час катастрофічно зростає ціна втрат в разі нештатного функціонування або зниження надійності систем обробки і передачі інформації. З підвищенням значущості і цінності інформації, відповідно зростає і важливість її захисту. Одним із можливих способів захисту інформації при її передачі та зберіганні є криптографічний захист.

Особливої уваги потребують *державні інформаційні ресурси (ДІР)* – інформація, яка є власністю держави та необхідність захисту якої визначено законодавством. Серед всього спектру методів захисту ДІР особливе місце займають саме криптографічні

методи [11, 31, 32, 41]. На відміну від інших методів, вони спираються лише на властивості самої інформації і не використовують властивості її матеріальних носіїв, особливості вузлів її обробки, передачі і зберігання. Широке використання і постійне збільшення об'єму інформаційних потоків викликає постійне зростання інтересу до криптографії. Останнім часом збільшується роль програмних криптографічних засобів ЗІ, які не потребують великих фінансових витрат порівняно з апаратними криптосистемами. Сучасні методи шифрування гарантують надійний ЗІ, але завжди є імовірність знаходження нових методів криптоаналізу, які дозволять послабити стійкість криптоалгоритмів.

Модель порушника в державних ІКС

Абстрактна модель порушника (attacker`s abstract model) – це формалізований (або неформалізований) опис можливих дій порушника *(ненавмисного* чи навмисного, так званого *зловмисника),* який складається на основі аналізу типу зловмисника, рівня його повноважень, знань, теоретичних та практичних можливостей. Відповідно до загальноприйнятих міжнародних позначень, порушника будемо називати *Євою (від англ. Eavesdropper - підслуховувач).*

Взагалі, порушників прийнято поділяти на зовнішніх і внутрішніх. До *внутрішніх* належать: співробітники підприємства-власника ІКС; користувачі ІКС, які можуть наносити шкоду ДІР як ненавмисно, так і навмисно; технічний персонал, який обслуговує будівлі і приміщення підприємства (електрики, сантехніки, прибиральниці тощо); персонал, який обслуговує технічні засоби (інженери, техніки). *Зовнішні порушники* – це сторонні особи, які знаходяться поза контрольованою зоною організації або не авторизовані для використання даної ІКС. Це означає, що вони не мають в ІКС облікового запису і згідно системної політики безпеки взагалі не можуть працювати у цій ІКС. Приклад зовнішніх порушників: відвідувачі, які можуть завдати шкоди навмисно або через незнання існуючих обмежень; кваліфіковані хакери; особи, яких найняли конкуренти для отримання необхідних ДІР; порушники пропускного режиму.

Основною метою Єви є НСД до ДІР, що циркулюють в ІКС, з різною ціллю. Виключенням є випадок, коли Єва ненавмисно реалізує НСД – у такому випадку вона є порушником (ненавмисним), але не зловмисником. Особливу небезпеку можуть нести порушники, які знаходяться під впливом: кримінальних угрупувань; бізнесових структур; політичних організацій; спецслужб тощо.

Кваліфікація порушника (attacker qualification) – сукупність певних знань і вмінь порушника, які він використовує для реалізації НСД до ІКС. Можна відзначити кілька типів кваліфікації порушників, що несуть ймовірну загрозу ДІР:

1) Єва володіє інформацією щодо функціональних особливостей ІКС взагалі, уміє користуватися штатними засобами;

2) Єва має високий рівень знань і досвід роботи в технічному обслуговуванні аналогічних ІКС;

3) Єва володіє високим рівнем знань в галузі обчислювальної техніки (зокрема, криптографії, теорії алгоритмів та паралельних обчислень тощо) і програмування на мовах розробки ПЗ ІКС чи її аналога;

4) Єва має доступ до глобальних обчислювальних мереж, суперкомп'ютера чи квантового комп'ютера, за допомогою якого може реалізувати, наприклад, атаку повного перебору на ІКС, використовуючи відомі квантові алгоритми Шора, Гровера [33, 40] тощо.

Можливості порушника (attacker ability) щодо впливу на ІКС можна представити у вигляді такої ієрархічної класифікації: 1) Єва має можливість запуску певного обмеженого набору ПЗ, що реалізує певні функції з обробки ДІР; 2) Єва може створювати власне ПЗ та модифікувати існуюче, що дозволить створити нові функції обробки ДІР і подальшого одержання частини необхідної Єві інформації; 3) Єва має змогу управляти функціонуванням ІКС, тобто безпосередньо впливати на ПЗ, склад та конфігурацію її технічного забезпечення; 4) Єва має весь обсяг можливостей легітимних користувачів (по аналогії з порушником будемо називати їх Алісою та Бобом – іншими словами – користувач А та Б) – може розробляти та впроваджувати в експлуатацію технічні засоби ІКС, а також інтегрувати власні технічні засоби з метою подальшого отримання ДІР.

За часом дії порушників можна класифікувати таким чином: 1) Єва діє у процесі функціонування ІКС (під час роботи компонент системи); 2) Єва діє у період неактивності ІКС (у неробочий час, під час планових перерв у її роботі, перерв для обслуговування та ремонтів і т.д.); 3) Єва діє як у процесі функціонування, так і в період неактивності компонент ІКС.

За місцем дії: 1) Єва не має доступу на контрольовану територію організації-власника ІКС; 2) Єва діє з контрольованої території без доступу до будівель та споруд, де знаходиться і функціонує ІКС; 3) Єва знаходиться усередині приміщень, але без доступу до технічних засобів ІКС; 4) Єва має доступ до робочих місць кінцевих користувачів (операторів) ІКС; 5) Єва має доступ у зону даних (баз даних, архівів і т.п.) ІКС; 6) Єва має доступ у зону управління засобами забезпечення безпеки ДІР, що циркулюють в ІКС організації.

Цілі порушника (attacker target) – це створення нових та підвищення ефективності існуючих методів аналізу стійкості класичних криптографічних засобів захисту ДІР. Підґрунтям цілеспрямованої реалізації Євою НСД до ДІР ІКС є найчастіше корисливі мотиви, хоча іноді буває бажання самовираження чи нанесення моральної шкоди Алісі та Бобу.

Єва може використовувати *сукупність релевантних знань, умінь та навиків*, для прикладу: досконале знання *математичного апарату* дозволить їй створити нові методи криптоаналізу відповідно до існуючого рівня криптографічного захисту ДІР; знання *мов програмування (програмної інженерії)* дозволить Єві реалізувати створені методи криптоаналізу, а також модифікувати існуюче ПЗ Аліси та Боба; знання *методів соціального інжинірингу* теоретично дозволить Єві без грунтовних знань математики та програмування обійти будь-які системи захисту ДІР (не лише криптографічні).

За характером дій порушників можна класифікувати так: 1) Єва – "випадковий порушник", що

помилково, ненавмисне і несвідомо порушив політику безпеки ІКС в процесі виконання свої посадових обов'язків чи іншої службової діяльності; 2) Єва – "терплячий порушник" безпеки, що порушив політику безпеки певного сегменту чи усієї ІКС свідомо, навмисно, але без рішучих дій, маскуючись, підбираючи атрибути доступу Аліси та Боба з метою подолання засобів управління доступом тощо; 3) Єва – "рішучий зловмисник", що має на меті порушити одну із властивостей ДІР, що циркулюють в ІКС. Вона прагне подолати усі існуючі засоби обмеження доступу і отримати можливість безпосереднього доступу до ДІР з метою втручання у роботу ІКС, модифікації, знищення чи отримання необхідних ДІР; 4) Єва – "віддалений порушник", що аналізує технічні канали витоку інформації, впливає віддалено за допомогою спеціальних засобів на локальні та розподілені ІКС, включаючи технології VPN, Wi-Fi, WiMAX тощо.

Для більш детальної побудови абстрактної моделі порушника, виходячи із конкретної ІКС, рекомендується також класифікувати порушників за такими ознаками:

– за підготовкою до подолання системи фізичного захисту ІКС (Єва може бути по різному підготовлена для подолання систем фізичного захисту, що може відіграти ключову роль у деяких випадках);

– за інформованістю про об'єкт атаки (різний рівень інформованості Єви про ІКС впливатиме на правильність вибору методів та засобів, і, як наслідок, на результат реалізації НСД);

– за використовуваними методами та засобами (тобто, в залежності від використовуваного інструментарію Єві буде необхідно використати певні методи та засоби, що будуть індивідуальними у більшості випадків реалізації НСД до ІКС, у яких циркулюють ДІР).

Визначення конкретних характеристик можливих порушників є значною мірою суб'єктивним. Модель порушника, що побудована з урахуванням особливостей конкретної предметної галузі і технології обробки інформації, може бути подана перелічуванням кількох варіантів його образу. Кожний вид порушника має бути схарактеризований згідно з класифікаціями, зазначеними вище. Всі наведені характеристики мають бути оцінені певним чином – кількісно чи якісно. Однак, при формуванні моделі порушника на її виході обов'язково повинні бути визначені: імовірність реалізації тієї чи іншої загрози, своєчасність виявлення і відомості про порушення.

Слід також звернути увагу на те, що всі кіберзлочини здійснюються людиною. Користувачі ІКС є її складовою, необхідним елементом. З іншого боку, вони є основною причиною і рушійною силою порушень і злочинів. Отже, питання безпеки захищених ІКС фактично є питанням людських відносин та людської поведінки.

Проблеми забезпечення безпеки ДІР

На сьогоднішній день існує багато алгоритмів шифрування, серед яких зустрічаються достатньо вдалі та широко використовувані, що розроблені не тільки спецслужбами, а й приватними особами. Їх опис можна знайти у багатьох наукових джерелах [2, 10, 15-17, 22, 25, 34-37].

Взагалі "*криптографія*" – грецьке слово, що походить від слів kryptos (таємний, схований) та graphy (запис) і включає методи і засоби забезпечення перетворення даних з метою маскування (шифрування) змісту інформації для гарантування конфіденційності та цілісності, а криптоаналіз, відповідно, орієнтований на зламування шифротекстів (шифрів).

Галузі застосування криптографії: безпечний зв'язок: веб-трафік: HTTPS, бездротовий трафік: 802.11i WPA2 (WEP), GSM, Bluetooth; шифрування файлів на диску: EFS, TrueCrypt; захист контенту (DVD, Blu-Ray): CSS, AACS; аутентифікація користувачів тощо.

Шифротекст є даними, представленими в зашифрованій формі і мають прихований семантичний зміст, який утворюються після шифрування (криптографічного перетворення) відкритого тексту (з неприхованим семантичним змістом). Зародження криптографії почалося з глибокої давнини, з якої до нас дійшов ряд систем шифрування, які швидше за все з'явилися одночасно з писемністю в 4 тис. до н. е. Методи секретного переписування були винайдені незалежно в багатьох стародавніх суспільствах (Єгипет, Шумер, Китай).

Шифрування – оборотне перетворення даних, з метою приховання інформації, *дешифрування* – зворотній процес, що полягає у відновленні первинних (до шифрування) даних. Проте, у сучасній літературі [10] можна знайти інші визначення: під шифруванням розуміється синтез процесів зашифрування і розшифрування, а от дешифрування – це відновлення вхідного тексту без знання ключа (тобто, це процес злому шифру – криптоаналіз). Єдиної думки сьогодні не існує, можливу дану ситуацію виправить прийняття національного стандарту у галузі криптографії.

Крім забезпечення конфіденційності ДІР, криптографія застосовується для розв'язання таких задач, як:

– перевірка справжності (аутентифікація). Одержувач може встановити відправника, а зловмисник не може під нього маскуватися;

– цілісність. Отримувач може перевірити несанкціоновану модифікацію в тексті, а зловмисник не може видати підробний текст за справжній;

– не заперечення авторства. Відправник не може в подальшому заперечувати відсилання даних.

У сучасній криптографії можна виділити такі базові розділи: 1) Симетрична (з секретним ключем) криптографія; 2) Асиметрична (з відкритим ключем) криптографія; 3) Квантова криптографія.

Симетрична криптографія [14, 32, 41] – це сукупність криптографічних методів, у яких використовується один секретний ключ для зашифрування і розшифрування.

Асиметрична криптографія [14, 32, 41] – це сукупність криптографічних методів, у яких використовуються роздільні ключі для реалізації процесу зашифрування і розшифрування – відкритий і секретний. У таких методах секретність повідомлень грунтується на складності обчислення ключа за деякою функціонально залежною від нього інформацією, що передається, як правило, різними каналами зв'язку.

Квантова криптографія [3, 8, 30, 39] – наука, що вивчає методи захисту систем зв'язку і базується на постулатах квантової механіки, об'єкти якої (здебільшого це фотони, хоча, в принципі, можуть використовуватись і інші носії) забезпечують процеси безпечної передачі інформації.

Криптосистема – це алгоритм плюс усі можливі відкриті тексти, шифротексти і ключі. Алгоритм вважається обчислювально безпечним (чи, як іноді називають, криптостійкими), якщо він не може бути зламаний (розкритий) з використанням доступних обчислювальних ресурсів зараз чи у майбутньому [14, 29]. З огляду на це, для визначення обчислювальної стійкості використовують потужні сучасні GRID системи, та інші обчислювальні мережі (які, до речі, є загальнодоступними в мережі Інтернет і приєднатися до них може будь-який користувач).

Гібридна криптосистема – криптосистема, що базується на методах асиметричної і симетричної криптографії, при цьому криптографічна система з відкритим ключем задіюється тільки для управління загальними ключами, які потім використовуються в традиційних криптосистемах із секретним ключем.

Під *комбінованою криптографічною системою захисту інформації* у даній роботі будемо розуміти сукупність взаємопов'язаних компонентів, серед яких елементи симетричної, асиметричної і квантової криптографії, спрямованих на забезпечення захищеної передачі ДІР.

Відповідно до роботи [29] для сучасних криптографічних систем захисту інформації існують такі загальні вимоги:

– шифротекст повинен піддаватися читанню тільки при наявності ключа;

– число операцій, необхідних для визначення ключа шифрування, за фрагментом шифротексту і відповідного йому відкритого тексту, повинно бути не менше загального числа можливих ключів;

– число операцій, необхідних для розшифровування шляхом перебору всіх можливих ключів (лобова атака), повинно мати строгу нижню оцінку і виходити за межі можливостей сучасних та перспективних комп'ютерних систем та мереж;

– знання алгоритму шифрування не повинно впливати на надійність криптографічного захисту;

– незначна зміна ключа повинна приводити до істотної зміни шифротексту;

– структурні елементи алгоритму шифрування повинні бути незмінними;

– довжина шифрованого тексту повинна бути близькою довжині відкритого тексту;

– не повинно бути простих і легко встановлюваних залежностей між ключами, що використовуються в процесі шифрування;

– алгоритм повинен допускати, як програмну, так і апаратну реалізацію, при цьому зміна довжини ключа не повинна вести до якісного погіршення алгоритму шифрування.

Виходячи із [29, 32] можна сформулювати основні принципи криптографії:

1) Принцип рівної міцності захисту. На шляху від одного законного власника до іншого ДІР можуть захищатись різними способами в залежності від загроз, що виникають. Так утворюється ланцюг захисту ДІР з ланками різного типу. Противник прагне знайти найслабкішу ланку, щоб з найменшими витратами добратися до інформації. Законні власники повинні враховувати це у своїй стратегії захисту ДІР криптографічними методами: безглуздо робити якусь ланку дуже міцною, якщо є слабкіші ланки.

2) Принцип доцільності захисту. На сучасному рівні технічного розвитку засоби зв'язку, засоби перехоплення повідомлень, а також засоби захисту ДІР вимагають занадто великих витрат. Тому, існує проблема співвідношення вартості ДІР, витрат на їх захист та витрат на її здобування. Перш ніж захищати ДІР криптографічними методами, треба відповісти на два питання:

– Чи отримає противник внаслідок атаки ДІР, що будуть більш цінними, ніж вартість самої атаки?

– Чи є ДІР, які захищає її власник, більш цінними, ніж вартість захисту? Відповідь на ці два питання визначає доцільність захисту й вибір підходящих засобів криптографічного захисту.

3) Принцип використання ключа. Розробка хорошого шифру – справа надзвичайно трудомістка. Тому, бажано збільшити термін життя цього шифру і використовувати його для шифрування якнайбільшої кількості повідомлень. Але при цьому виникає небезпека, що противник вже зламав шифр і вільно читає шифровані повідомлення. Саме тому в сучасних шифрах використовують ключі. *Ключем* в криптографії називають змінюваний елемент шифру, який застосовується для шифрування конкретного повідомлення. При цьому вважають, що сам шифр (крім ключа) є відомим противнику і доступним для вивчення. Оригінальність подання повідомлення забезпечується тільки періодично змінюваним ключем. Знання ключа дозволяє швидко та просто відновити початковий текст. Без знання ключа дешифрування тексту має бути практично недосяжним.

4) Принцип стійкості шифру. Здатність шифру протидіяти різноманітним атакам на нього називається стійкістю шифру. З математичної точки зору проблема отримання строго доведених оцінок стійкості для будь-якого шифру ще не вирішена. Ця проблема відноситься до проблем нижніх оцінок обчислювальної складності задачі, ще нерозв'язаних математично. Тому, стійкість конкретного шифру оцінюється шляхом різноманітних спроб його зламування, а отримані результати оцінюють в залежності від кваліфікації криптоаналітиків, що атакують цей шифр.

5) Принцип Керкхоффса. Стійкість сучасного шифру має визначатись, в першу чергу, ключем. Зміст цього принципу полягає в тому, що захищеність інформації не повинна залежати від таких чинників, які важко змінити при появі загрози. При використанні ключів законним власникам ДІР легше перешкоджати противнику, оскільки міняти їх можна досить часто. Щоправда, тепер перед законними власниками виникає інша задача – як таємно обмінятись ключами перед тим, як обмінюватись шифрованими повідомленнями.

6) Принцип використання різноманітних шифрів. Не існує єдиного шифру, що підходить до всіх випадків. Вибір шифру залежить від особливостей інформації (може мати різний характер, тобто бути

документальною, телефонною, телевізійною, комп'ютерною тощо), від цінності інформації, від обсягів інформації, від потрібної швидкості її передачі, від тривалості захисту ДІР (державні та військові таємниці зберігаються десятками років, біржеві – декілька годин), від можливостей зловмисника (можна протидіяти окремій особі, можна протидіяти потужній державній структурі), а також від можливостей власників ДІР.

Проведений аналіз дозволив виділити такі ***актуальні проблеми забезпечення захисту ДІР:***

1) Загроза розкриття шифротекстів за допомогою сучасних обчислювальних технологій (суперкомп'ютер, квантовий комп'ютер, GRID-обчислення тощо).

2) Використання асиметричної криптографії базується на гіпотетичній неможливості розв'язання певного класу математичних задач, які, з огляду на розвиток сучасних обчислювальних потужностей, можуть бути розв'язаними у недалекому майбутньому.

3) Проблема розподілу ключів шифрування – ключі мають бути доставленими до легітимних користувачів в необхідний час і за умов суворої секретності – це зробити досить складно і здебільшого, зокрема в Україні, для вирішення цієї проблеми використовують не цілком надійні методи «довірених кур'єрів» (висока вартість та залежність від людського чиннику) та методи асиметричної криптографії.

4) Існуючі криптографічні засоби захисту ДІР [25] мають, як правило, закриту інфраструктуру, що ускладнює їх аналіз, та знижує об'єктивність оцінки їх ефективності.

Сучасні підходи до вирішення проблеми розподілу криптографічних ключів

Зважаючи на зростання об'ємів ДІР, варто констатувати той факт, що збільшуються вимоги до їх захисту, зокрема до забезпечення конфіденційності. Як уже зазначалось, конфіденційність забезпечується здебільшого криптографічними методами захисту, які постійно потребують удосконалення з огляду на розвиток криптоаналітичних засобів. Важливим елементом криптографії є управління ключовою інформацією (або управління ключами шифрування).

Управління ключами шифрування – це інформаційний процес, що включає в себе три елементи: *генерацію, накопичення та розподіл ключів.*

Генерація ключів ставить певні вимоги до генераторів псевдовипадкових послідовностей, які, відповідно до принципу Діріхле, мають кінцеве число станів, що повторюються через певний період [11, 14, 32].

Накопичення ключів є теж важливим процесом, зважаючи на що, не рекомендується записувати їх у відкритому вигляді на носії. Для підвищення рівня безпеки необхідно кожен ключ зашифровувати другим ключем, другий третім і т.д. Останній ключ (мастер-ключ) не зашифровується, а зберігається у захищеній ділянці носія.

Розподіл ключів шифрування між законними користувачами в умовах суворої секретності є однією з найважливіших проблем криптографії, яка особливо гостро постає в епоху глобальної інформатизації.

Системи захисту інформації з відкритим ключем. Одним з найпоширеніших методів розподілу ключів шифрування є ***використання класичної криптографічної схеми з відкритим ключем.*** Яскравим прикладом такої схеми є протокол Діфі-Хелмана (Diffie-Hellman) та цифровий конверт [8]. *Схема Діфі-Хелмана* дозволяє двом легітимним користувачам обмінятися секретним ключем через відкритий канал без попередньої зустрічі.

Схема цифрового конверту (digital envelope) передбачає такі дії: а) генерація сесійного (одноразового) ключа; б) зашифровування сесійним секретним ключем; в) зашифровування відкритого ключа отримувача – це і буде цифровим конвертом; г) зашифроване повідомлення та цифровий конверт передаються легітимному користувачеві; д) отримувач розшифровує цифровий конверт секретним ключем і розшифровує повідомлення отриманим сесійним ключем. Основними недоліками таких схем є обчислювальна стійкість, притаманна усій асиметричній криптографії, а також низька швидкість криптообробки (для прикладу, найшвидша реалізація алгоритму RSA є повільнішою за стандартний алгоритм симетричного шифрування мінімум на три порядки).

Загалом, асиметричні криптосистеми – ефективні системи криптографічного захисту даних, які також називають криптосистемами з відкритим ключем. У таких системах для зашифровування даних використовується один ключ, а для розшифровування – інший ключ (звідси і назва – асиметричні). Перший ключ є відкритим і може бути опублікованим для використання усіма користувачами системи, які зашифровують дані. Розшифровування даних за допомогою відкритого ключа неможливе. Для розшифровування даних отримувач зашифрованої інформації використовує другий ключ, який є секретним. Зрозуміло, що ключ розшифровування не може бути визначеним з ключа зашифровування.

Головне досягнення асиметричного шифрування в тому, що воно дозволяє людям, що не мають існуючої домовленості про безпеку, обмінюватися секретними повідомленнями (рис.1). Необхідність відправникові й одержувачеві погоджувати таємний ключ по спеціальному захищеному каналі цілком відпала. Прикладами криптосистем з відкритим ключем є *Elgamal* (названа на честь автора, Таxіра Ельгамаля), *RSA* (названа на честь винахідників: Рона Райвеста, Аді Шаміра і Леонарда Адлмана), згадана нами раніше *Diffie-Hellman* і *DSA* (Digital Signature Algorithm, винайдений Девідом Кравіцом) [41].

Рис.1. Типова схема асиметричної криптографії

Широке поширення асиметричних алгоритмів шифрування викликано необхідністю мати два ключі – відкритий для зашифрування (хоча у випадку

застосування асиметричного алгоритму з метою організації, наприклад ЕЦП, відкритий ключ може використовуватися для розшифрування) і закритий для розшифрування. Відповідно, вводячи поняття відкритого ключа, тобто ключа, потенційно відомого всім, позбулися необхідності вирішувати складне завдання обміну секретними ключами. Так, наприклад, в деяких випадках необхідність зберігати секретні ключі призводить до утворення великих обсягів статистичної інформації, що часом практично нездійсненне. Таке, зокрема, може статися при необхідності використання мережі Internet як середовища передачі даних і, одночасно, за бажання мати належний рівень безпеки.

Отже, маючи у своєму розпорядженні механізм розподілу відкритих ключів, можна послати ключ відкритими каналами зв'язку та встановити захищений канал передачі даних, хай навіть при цьому виникнуть проблеми забезпечення безпеки відкритих ключів. Зловмисник у разі такого обміну або при зберіганні ключів у відкритих довідниках намагається підмінити їх, що може призвести до встановлення помилкової зв'язку, і застосовувати їх замість легального користувача, чий відкритий ключ був скомпрометований. На практиці при застосуванні асиметричного алгоритму в ролі секретного ключа виступає саме знання секрету, а в ролі відкритого ключа – знання процедури обчислення односторонньої функції з секретом. Разом з тим необхідно відзначити, що стійкість більшості сучасних асиметричних алгоритмів базується на двох математичних задачах, які на даному етапі є важкообчислювальними навіть для методу "грубої сили": дискретне логарифмуванню в кінцевих полях; факторизація великих чисел тощо.

Оскільки на сьогоднішній день не існує ефективних алгоритмів розв'язання даних задач або їх розв'язок вимагає залучення великих обчислювальних ресурсів або тимчасових витрат, ці математичні задачі знайшли широке застосування в побудові асиметричних алгоритмів.

Квантовий розподіл ключів

Головною і беззаперечною перевагою квантового розподілу ключів (КРК) є забезпечення теоретико-інформаційної (безумовної, абсолютної) стійкості, яка не залежить від обчислювальних або інших можливостей потенційних зловмисників). Жоден з класичних традиційних методів розподілу ключів не здатен забезпечити теоретико-інформаційну стійкість ключа в процесі обміну між легітимними абонентами. Метод КРК включає в себе такі протоколи [3, 8, 30]: протоколи з використанням одиночних поляризованих фотонів; протоколи з використанням фазового кодування; протоколи з використанням переплутаних станів; протоколи зі станами "приманки".

Ідея використання квантових об'єктів для ЗІ була вперше запропонована у 1970 році Стефаном Вейснером – його гіпотеза полягала у можливості застосування елементарних квантових частинок для захисту грошових купюр. На той момент це вигляділо досить фантастично і Вейснер не знайшов підтримки у відомих вчених того часу. Проте, зовсім незабаром, уже в 1984 році Чарльз Беннет з компанії IBM та Жіль Брассар з Монреальського університету розвинули ідею Стефана Вейснера і запропонували перший протокол [30] квантової криптографії, що мав стати альтернативним і нетрадиційним вирішенням проблеми розподілу ключів шифрування. Даний протокол отримав назву ***BB84,*** він відноситься до квантових протоколів КРК з використанням одиничних поляризованих фотонів. Даний протокол полягає у тому, що відправник (Аліса) кодує і відправляє дані (рис.2), задаючи певні квантові стани, одержувач (Боб) реєструє ці стани (рис.3). Потім одержувач і відправник спільно обговорюють результати спостережень. Вкінці кінців з високою вірогідністю можна бути впевненим, що передані й прийняті кодові послідовності тотожні.

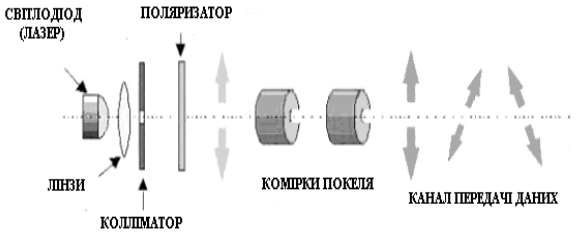

Рис.2. Схема передаючої сторони

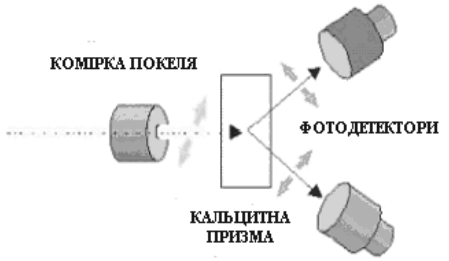

Рис.3. Схема приймаючої сторони

Обговорення результатів стосується помилок, внесених шумами або зловмисником, і навіть в найменшій мірі не розкриває змісту переданого повідомлення. Може обговорюватися парність повідомлення, але не окремі біти. Відкритий канал зв'язку не зобов'язаний бути конфіденційним, тільки аутентифікованим. Щоб обмінятися ключем за даним протоколом, Аліса та Боб виконують такі дії (детально описані в [3, 6]):

1. Аліса посилає Бобу біт, задаючи певні квантові стани – поляризацію в 0°, 45°, 90°, 135°. Відлік кутів можна вести від напрямку "вертикально догори" по годинниковій стрілці.

2. Боб користується двома аналізаторами: один розпізнає вертикально-горизонтальну поляризацію, інший – діагональну. Для кожного фотона Боб випадково вибирає один з аналізаторів і записує тип аналізатора та результат вимірів. Отриманий так званий сирий ключ з імовірністю ~ 75%. Тобто, він містить ~ 25% помилок.

3. Відкритим каналом зв'язку Боб повідомляє Алісу, які аналізатори використалися але не повідомляє, які конкретно результати були отримані внаслідок вимірювання.

4. Аліса тим же відкритим каналом зв'язку повідомляє Бобу, які аналізатори він вибрав правильно. Далі, ті фотони, для яких Боб невірно вибрав аналізатор, відкидаються.

5. Для виявлення перехоплення Аліса й Боб вибирають випадкову ділянку ключа й порівнюють її відкритим каналом зв'язку. Якщо відсоток помилок

великий, то він може бути віднесений на рахунок зловмисника (Єви) і процедура повторюється спочатку.

З технологічної точки зору як джерело світла може використовуватися світловипромінюючий діод або лазер, у якості детекторів здебільшого застосовують лавинні фотодіоди, а у якості провідників використовують або атмосферу, або оптоволоконні кабелі (з огляду на результати експериментів у цій галузі , рекомендується застосовувати одномодове оптоволокно, що забезпечує стійкість поляризаційних станів фотонів).

Основними задачами КРК є генерація та розподіл ключів шифрування між двома абонентами, що з'єднані квантовим та класичним каналами зв'язку. У більшості протоколів з одиничними поляризованими фотонами використовуються 4 згадані поляризовані стани фотонів, що передаються квантовим каналом зв'язку. Пошук та виправлення помилок виконується з використанням відкритого класичного каналу, який не повинен бути конфіденційним, тільки аутентифікованим. Для виявлення факту дій зловмисника використовується ***процедура корекції помилок***, а для забезпечення безумовної стійкості використовується класична ***процедура підсилення секретності*** [8].

Ефективність протоколу BB84 з кубітами в ідеальних умовах дорівнює 50%. Під ***ефективністю*** у квантовій криптографії будемо вважати відношення кількості фотонів, що використовуються для генерації ключа до загальної кількості переданих фотонів. Крім того, на даний момент запропоновано узагальнення протоколу BB84 на багаторівневі квантові системи (так званий протокол BB84 з кудитами). Цей протокол має значно більшу інформаційну місткість та стійкість до некогерентних атак, але його складніше реалізувати з технічної точки зору.

Як вже зрозуміло із опису протоколу, вихідними даними КРК є ключова послідовність, яка може бути використана для подальшого шифрування даних. До вищезгаданого типу протоколів КРК, крім BB84, відповідно до [39] відносяться також: протокол з шістьома станами; протокол 4+2; протокол Гольденберга-Вайдмана; протокол Коаші-Імото.

Протокол з шістьома станами передбачає використання чотирьох станів, аналогічних протоколу BB84 і додатково вводяться ще два можливих напрямки поляризації – право-циркулярний та лівоциркулярний. Такі зміни з одного боку зменшують кількість інформації, що може бути отримана зловмисником, а з іншого боку ефективність протоколу також зменшується (до 33%). Також запропоновано узагальнення протоколу з шістьома станами на багаторівневі квантові системи. Даний протокол має дещо більшу інформаційну місткість та значно більшу стійкість до атаки "перехоплення – повторної посилки" кудитів.

Протокол 4+2 є перехідним між BB84 та B92. У ньому використовуються чотири квантових стани для кодування "0" та "1" у двох базисах. Стани в кожному базисі вибираються неортогональними, крім того, стани в різних базисах також мають бути попарно неортогональними. Для протоколу 4+2 характерна менша кількість помилок відносно протоколу BB84 для кубітів і менша кількість корисної інформації, що може отримати зловмисник, але одночасно відбувається й зменшення відносної ефективності даного протоколу.

У *протоколі Гольденберга-Вайдмана* кодування "0" та "1" виконується за допомогою двох ортогональних станів. Кожен з цих двох станів є суперпозицією двох локалізованих нормалізованих хвильових пакетів. Для захисту проти атаки «перехоплення – повторної посилки» використовується випадковий час відправлення пакетів.

Модифікований варіант протоколу Гольденберга-Вайдмана – це *протокол Коаші-Імото*, удосконалений тим, що замість випадкового часу відправлення пакетів використовується асиметризація інтерферометра, тобто світло розбивається у нерівних пропорціях між довгим і коротким плечами інтерферометра.

Першим вітчизняним дисертаційним дослідженням у галузі квантової криптографії є робота, що базується на статтях [26-30]. У даній праці виконано дослідження, що спрямовані на підвищення рівня захищеності електронних інформаційних ресурсів інформаційно-комунікаційних систем за рахунок удосконалення їх систем захисту квантовими складовими. Запропоновані автором квантові системи захисту інформації дозволяють досягнути ***теоретико-інформаційної стійкості при передачі ключа шифрування*** (з тієї точки зору, що квантовий прямий безпечний зв'язок, наприклад пінг-понг протокол, також може розглядатись як альтернативний метод розподілу ключів).

Наступний тип КРК – ***протоколи квантового розподілу ключів з використанням фазового кодування*** [39]. Найвідомішим представником даного типу протоколів є B92 – концептуально найпростіший квантовий протокол, в якому використовуються будь-які два неортогональні поляризовані стани фотонів, а виявлення факту атаки зловмисника відбувається аналогічно процедурам, описаним вище для протоколу BB84. Ефективність даного протоколу становить 25%, тому він не є практично важливим протоколом.

Усі вищенаведені протоколи КРК ґрунтуються на принципі квантової механіки, що полягає у ***неможливості розрізнити абсолютно надійно два неортогональні квантові стани*** [33, 40], а їх захищеність базується на ***теоремі про заборону клонування невідомого квантового стану*** [9].

Протокол Екерта (він же *E91*) [39], відноситься до КРК з використанням ***переплутаних станів (кореляції)***, властивості яких детально описані в роботах [19, 26-28]. Такого типу кореляція полягає у тому, що квантово-механічні системи (в тому числі і розділені у просторі) можуть знаходитися у взаємозалежному стані, тому вимірювання обраної величини однієї із систем визначить результат вимірювання цієї ж величини на іншою системою. Під час передавання інформації за протоколом E91, перехоплення одного із фотонів пари не дає зловмиснику ніякої корисної інформації. Крім того, запропоновано узагальнення схеми Екерта на багатовимірні квантові системи, що значно збільшує інформаційну місткість протоколу.

Іншими словами, якщо Аліса та Боб не збираються використати отриманий ними ключ

відразу, то перед ними виникає нова проблема – як зберегти ключ у секреті?! У 1991 р. Артур Екерт запропонував протокол, що дозволяє вирішити обидві ці проблеми – поширення й зберігання ключа. Протокол Екерта заснований на ефекті EPR [40]. Ефект EPR виникає, коли сферично симетричний атом випромінює два фотони в протилежних напрямках убік двох спостерігачів. Фотони випромінюються з невизначеною поляризацією, але в силу симетрії їхньої поляризації завжди протилежні. Такі стани двох фотонів називаються зчепленими (переплутаними).

На основі ефекту EPR Екерт запропонував криптосхему, що гарантує безпеку пересилання й зберігання ключа. Відправник генерує деяку кількість EPR фотонних пар. Один фотон з кожної пари він залишає для себе, другий посилає своєму партнерові. При цьому, якщо ефективність реєстрації близька до одиниці, при одержанні відправником значення поляризації "1", його партнер зареєструє значення "0" і навпаки. Ясно, що в такий спосіб партнери щораз, коли потрібно, можуть одержати ідентичні псевдовипадкові кодові послідовності. Практично реалізація даної схеми проблематична через низьку ефективність реєстрації й виміру поляризації одиночного фотона. Неефективність реєстрації є платою за таємність. Варто враховувати, що при роботі в однофотонному режимі виникають чисто квантові ефекти. При горизонтальній поляризації й використанні вертикального поляризатора результат очевидний – фотон не буде зареєстрований. При 45 поляризації фотона й вертикальному поляризаторі ймовірність реєстрації 50%. Труднощі також полягають у тому, що в цей час не всі зчеплені стани піддаються виміру, не говорячи вже про створення ідеальних ємностей, для зберігання фотонів (так званої квантової пам'яті).

Протокол SARG04 [8] має невеликі відмінності від оригінального протоколу BB84, які не стосуються його "квантової" частини (тобто тут він співпадає с протоколом BB84), а стосуються тільки "класичної" процедури просіювання ключа, яка виконується в цих протоколах після квантової передачі. Таке удосконалення дозволяє підвищити стійкість протоколу до атаки розділення кількості фотонів (photon number splitting attack). Також при реалізації протоколів на реальному обладнанні SARG04 має більш високу швидкість генерації ключа і може виконуватися для більших відстаней між легітимними абонентами, ніж протокол BB84.

Протоколи зі станами "приманки" (decoy states protocols) є удосконаленим варіантом протоколу BB84, у якому відправник, шляхом заміни підмножини імпульсів, вводить так звані приманки. Як показують практичні експерименти, даному типу протоколів характерний більш високий рівень безпеки, ніж у BB84. Крім того, такі протоколи відзначаються стійкістю проти атаки розділення кількості фотонів. До явних переваг протоколів зі станами "приманки" також можна віднести і збільшення довжини каналу за рахунок лінійної залежності від втрат у каналі. Проте, без попередньої аутентифікації користувачів на таких протоколах не можливо побудувати завершене повноцінне рішення проблеми розподілення криптографічних ключів.

Отже, проаналізувавши протоколи КРК – можна підбити певні підсумки і виділити переваги та недоліки. До переваг можна віднести таке:

– протоколи КРК дозволяють завжди виявити атаку пасивного перехоплення (eavesdropping), так як підключення зловмисника вносить до каналу значно більший рівень помилок порівняно з природнім рівнем;

– безумовна (теоретико-інформаційна) безпека, що дозволяє використати абсолютно секретний ключ для подальшого шифрування відомими класичними симетричними системами – це відповідно збільшить рівень захищеності даних суто класичних систем. Також, можливий синтез КРК з шифром Вернама (одноразовим блокнотом) [6], що в поєднані зі стійкою схемою аутентифікації дасть абсолютно стійку систему обміну повідомленнями.

До суттєвих недоліків квантових протоколів розподілу ключів відносяться:

– система, побудована на КРК не може слугувати повноцінним завершеним рішенням (без попередньої аутентифікації користувачів) проблеми розподілу ключів;

– обмеження довжини квантового каналу, тобто неможливість підсилення без втрати квантових властивостей;

– швидкість передачі інформації квантовим каналом суттєво зменшується зі збільшенням довжини каналу і на відстанях порядку 100 км дорівнює декільком бітам за секунду;

– проблеми реєстрації фотонів – ефект "темнового шуму" (так званих темнових відліків);

– залежність каналу від зовнішнього впливу (наприклад, від погодних умов, середовища тощо), особливо при використанні поляризаційних станів фотонів;

– складність технічної реалізації протоколів з багатовимірними квантовими системами;

– деполяризація фотонів (неможливість підсилення за допомогою повторювачів, як у класичних системах) навіть при використанні стійкого до деполяризації одномодового оптоволокна – це головний недолік систем, у яких ключі шифрування кодуються у поляризаційні стани фотонів (кубітів чи кудитів);

– висока ринкова ціна комерційних рішень (близько 100-150 тис. доларів США [24]), що робить їх недоступним для більшості вітчизняних користувачів.

Інші методи розподілу ключів

У нашій країні проблема розподілу ключів шифрування (key distribution problem) має два практичних варіанти вирішення – це, по-перше, застосування ***асиметричної криптографії***, що використовується у вітчизняній банківській системі. Другим варіантом є використання **довірених кур'єрів,** що досить поширено у галузі державного управління. Крім того, на ряду з цими методами та КРК, існують і інші підходи до вирішення зазначеної проблеми [30], які, хоч і не знайшли широкого застосування у нашій країні, проте наукові дослідження та практичне використання доводять їх ефективність та перспективи. До таких методів відносять:

1) використання ***класичної криптографічної схеми з теоретико-інформаційною стійкістю.*** Для її

реалізації потрібно канал з перешкодами (помилками), наприклад, зв'язок із супутником. У результаті і легітимні користувачі, і зловмисник отримають різні послідовності бітів. Далі абоненти, виконуючи спеціальну процедуру advantage distillation, узгоджують свої послідовності відкритим аутентифікованим каналом (відкидають більше 90% бітів) і виконують процедуру підсилення секретності (privacy amplification). Зловмисник не може виконати аналогічні дії, так як його послідовність відрізняються від усіх послідовностей легітимних користувачів. На практиці сьогодні досить складно знайти канал з таким високим рівнем помилок, до того ж, ефективність такої схеми є вкрай низькою – 1-5%;

2) застосування ***класичної симетричної криптографічної схеми з обчислювальною стійкістю.*** Дана схема потребує наявності у абонентів попередньо встановленого ключа, тобто вона може розглядатися лише як схема для збільшення довжини ключа, а не безпосередньо його розподілу. До того ж, обчислювальна стійкість вказує на залежність від рівня розвитку сучасних криптоаналітичних технологій, що безперечно є недоліком.

Сучасні методи генерування криптографічних ключів

Випадкові числа (ВЧ) – це така послідовність чисел, для якої неможливо передбачити наступне число, навіть якщо відомі попередні. Псевдови-падкові числа (ПВЧ) – це така послідовність чисел, яка має властивості випадкових чисел, проте кожне наступне число обчислюється за певною формулою. Псевдовипадкова двійкова послідовність – частковий випадок ПВЧ, у якому елементи приймають два можливі значення «0» і «1» (інколи цими значеннями є «–1» та «+1») [20].

Для отримання таких чисел використовують обчислювальний або фізичний пристрій, який спроектовано для генерації послідовності номерів чи символів, що не відповідають будь-якому шаблону – генератор випадкових чисел (ГВЧ). Деякі вчені вважають, що немає істино випадкових генераторів, а є лише ГПВЧ, відповідно і результатом їх роботи є ПВЧ, а не ВЧ. Хоча псевдовипадкова послідовність на перший погляд може здатися, позбавленою закономірностей, проте будь-який ГПВЧ з кінцевим числом внутрішніх станів повториться після дуже довгої послідовності чисел (що доводиться за допомогою принципу Діріхле [20, 30]). Основним завдання розробників таких генераторів є забезпечення якомога більшого періоду повторюваності.

Внаслідок швидкого розвитку методів статистичного моделювання і криптографії, галузь застосування ГВЧ істотно розширилася. Можливість реалізації ГВЧ для зазначених застосувань була забезпечена, з одного боку, розвитком теорії ймовірностей і математичної статистики, а з іншого – становленням радіоелектроніки та створенням обчислювальних засобів, що дозволили швидко проводити складні математичні обчислення. ГВЧ використовуються в існуючих криптосистемах для генерації ключової інформації і визначення ряду параметрів криптосистем.

Відповідно до, згаданого у першому пункті даної роботи, принципу Керкгоффса стійкість криптографічного алгоритму не має залежати від архітектури алгоритму, а має залежати тільки від ключів. Іншими словами, при оцінці надійності шифрування необхідно вважати, що супротивник знає все про систему шифрування, що використовується, крім ключів. З огляду на це, досить важливою задачею є забезпечення секретності такої критично важливої ланки криптосистеми як ключ. Однією із умов секретності є статистична незалежність між різними послідовностями (тобто ключами).

Будь-які послідовності, породжувані ГВЧ (або ГПВЧ) безпосередньо для криптографічних цілей, підлягають обов'язковому тестуванню. Тестування псевдовипадкових послідовностей – це сукупність методів та засобів визначення міри близькості заданої псевдовипадкової послідовності до випадкової. У якості критерію зазвичай виступає наявність рівномірного розподілу, великого періоду, рівної частоти появи однакових підрядків тощо.

Існують такі *методи тестування* ПВЧ:

1) Графічні тести. До цієї категорії відносяться тести, результати яких відображаються у вигляді графіків, що характеризують властивості досліджуваної послідовності. Серед них: гістограма розподілу елементів послідовності; розподіл на площині; перевірка серій; перевірка на монотонність; автокореляційна функція; профіль лінійної складності; графічний спектральний тест та ін.

Проте, результати графічних тестів інтерпретуються безпосередньо людиною, тому висновки на їх основі можуть бути неоднозначними і суб'єктивними (людський чинник).

2) Статистичні тести [30]. На відміну від графічних, статистичні тести видають чисельну характеристику ПВЧ і дозволяють однозначно сказати, чи пройдений конкретний тест, чи ні. Сьогодні найбільш відомими і використовуваними є такі статистичні тести: добірка тестів Д. Кнута, DIEHARD, CRYPT-X, NIST STS [1, 7], FIPS.

Вимоги до генерування ПВЧ:

Одне з перших формулювань деяких основних правил для статистичних властивостей періодичних псевдовипадкових послідовностей була представлена Соломоном Голомбом. Три основних правила отримали популярність як постулати Голомба [30]:

1. Кількість «1» у кожному періоді має відрізнятися від кількості «0» не більш, ніж на одиницю.

2. У кожному періоді половина серій (з однакових символів) повинна мати довжину один, одна чверть повинна мати довжину два, одна восьма повинна мати довжину три і т.д. Більше того, для кожної з цих довжин має бути однакова кількість серій з «1» і «0».

3. Припустимо, у нас є дві копії однієї і тієї ж послідовності періоду p, зсунуті відносно один одного на деяке значення d. Тоді для кожного d, $0 \le d \le pl$, ми можемо підрахувати кількість узгоджень між цими двома послідовностями Ad, і кількість неузгодженостей Dd. Коефіцієнт автокореляції для кожного d визначається співвідношенням $(Ad - Dd)/p$ і ця функція автокореляції приймає різні значення в міру того, як d проходить всі допустимі значення. Тоді, для будь-якої

послідовності, що задовольняє правилом 3, автокореляційна функція повинна приймати лише два значення.

Серед існуючих методів захисту інформації саме для криптографічних методів доцільно використовувати ГПП (у процесі формування ключів). Секретні ключі являють собою основу симетричних криптографічних перетворень, для яких стійкість хорошої шифрувальної системи визначається лише секретністю ключа. Однак, на практиці створення, розподіл і зберігання ключів – це задачі технічно не складні, проте потребують серйозних фінансових витрат. Основна проблема класичної криптографії довгий час полягала в труднощах генерації непередбачуваних двійкових послідовностей великої довжини із застосуванням короткого випадкового ключа. Саме для її вирішення широко використовуються ГПП.

Найважливіша характеристика ГПП – інформаційна довжина періоду, після якого числа або почнуть просто повторюватися, або їх можна буде передбачати. Ця довжина фактично визначає можливе число ключів системи і залежить від алгоритму отримання псевдовипадкових чисел. Необхідну довжину періоду визначає ступінь секретності даних: чим довший ключ, тим важче його підібрати. Однак не тільки довжина ключа гарантує його стійкість до злому.

Друга проблема полягає у визначенні принципів на підставі яких можна зробити висновок, що гамма конкретного ГПП є непередбачуваною. Поки у світі немає універсальних та практично перевірених критеріїв, що дозволяють стверджувати це! Невідома й загальна теорія криптоаналізу, яка могла б бути застосована для доказу, за винятком всезростаючої кількості конкретних способів аналізу, вироблених для різних практичних цілей. Інтуїтивно випадковість сприймається як непередбачуваність. Щоб гамма вважалася випадковою, як мінімум необхідно, щоб її період був дуже великим (проте, тут же виникає питання – «Який період є дуже великим, а який не дуже?»), а різні комбінації біт певної довжини рівномірно розподілялися по всій її довжині.

Отже, друга вимога до ряду полягає в підтвердженій статистично подібності його властивостей цієї випадкової вибірки. Кожен порядок елементів гами повинен бути так само випадковий, як і будь-який інший. Цю вимогу статистики можна тлумачити і як складність закону формування ряду ПВП. Практично, якщо за досить довгої реалізації цей закон розкрити не вдається ні на статистичному рівні, ні аналітично, то цим потрібно задовольнитися. Чим більша довжина ряду, що потребується, тим жорсткіше до нього вимоги.

І остання, *третя вимога, пов'язана з можливістю практичної реалізації генератора* у вигляді програми або електронного пристрою, швидкодією, необхідною для застосування в сучасних комунікаціях, а також зручністю його практичного використання.

Сучасні ефективні методи та засоби генерування ПВЧ.

Одним з перших був метод, запропонований в 1946 році Д. фон Нейманом [14]. Цей метод базувався на тому, що кожне наступне число в псевдовипадковою послідовності формувалося зведенням попереднього числа в квадрат і відкиданням цифр з обох кінців. Однак цей метод виявився ненадійним, і від нього швидко відмовилися.

Іншим методом є так званий конгруентний спосіб. *Лінійний конгруентний метод* – один з алгоритмів генерації ПВЧ. Застосовується в простих випадках і не має криптографічної стійкості [14]. Входить в стандартні бібліотеки різних компіляторів.

Цей алгоритм полягає в ітеративному застосуванні такої формули [20]:

$$x_{n+1} = (ax_n + c) \bmod m, \qquad (1)$$

де *a>0, c>0, m>0* – деякі цілочисельні константи. Отримана послідовність залежить від вибору стартового числа x_0 і при різних його значеннях виходять різні послідовності випадкових чисел. У той же час, багато властивостей послідовності x_j визначаються вибором коефіцієнтів у формулі і не залежать від вибору стартового числа. Ясно, що послідовність чисел, що генерується таким алгоритмом, періодична з періодом, що не перевищує m. При цьому довжина періоду дорівнює *m* тоді і тільки тоді, коли:

- НСД (*c, m*) = 1 (тобто *c* і *m* взаємно прості);
- *a* – 1 кратне *p* для всіх простих *p* – дільників *m*;
- *a* – 1 кратне 4, якщо *m* кратне 4.

Статистичні властивості одержуваної послідовності випадкових чисел повністю визначаються вибором констант *a* і *c* при заданій розрядності *e*. Для цих констант виписані умови, що гарантують задовільну якість отримуваних випадкових чисел.

BBS. Запропонований в 1986 році Ленор і Мануелем Блюм та Майклом Шубом, метод BBS полягає у використанні формули [5]:

$$x_{n+1} = x_n^2 \bmod M, \qquad (2)$$

де *M=p*q* є добутком двох великих простих чисел *p* і *q*.

На кожному кроці алгоритму вихідні дані отримуються з x_n шляхом взяття біту парності, або одного чи більше найменш значущих біт x_n. Два простих числа, *p* і *q*, повинні бути порівняні з третім за модулем 4 і НСД *(ц(p-1), ц(q-1))* повинен бути малим [26].

Цікавою особливістю цього алгоритму є те, що для отримання x_n не обов'язково вираховувати всі *n*–1 попередніх чисел, якщо відомий початковий стан генератора x_0 та чисел *p* і *q*; *n*-не значення може бути обчислено «напряму», використовуючи формулу (3):

$$x_n = x_n^{(2\wedge n) \bmod((p-1)(q-1))} \bmod M, \qquad (3)$$

Метод Фібоначчі. Цікавий клас ГПВЧ заснований на використанні послідовностей Фібоначчі. Класичний приклад такої послідовності {0, 1, 1, 2, 3, 5, 8, 13, 21, 34 ...} – за винятком перших двох її членів, кожен наступний дорівнює сумі двох попередніх [30]. Особливості розподілу випадкових чисел, що генеруються лінійним конгруентним алгоритмом, роблять неможливим їх використання в статистичних алгоритмах, що вимагають високої стійкості.

У зв'язку з цим, лінійний конгруентний алгоритм поступово втратив свою популярність, і його місце зайняло сімейство алгоритмів Фібоначчі, які можуть бути рекомендовані для використання в алгоритмах, критичних до якості випадкових чисел. У англомовній літературі датчики Фібоначчі такого типу

називають зазвичай «*Subtract-with-borrow Generators*» *(SWBG)* [16].

Найбільшу популярність датчики Фібоначчі отримали у зв'язку з тим, що швидкість виконання арифметичних операцій з числами зрівнялася зі швидкістю цілочисленної арифметики, а датчики Фібоначчі природно реалізуються у дійсній арифметиці.

Лінійний регістр зсуву зі зворотним зв'язком. Зсувний регістр зі зворотним зв'язком (LFSR – Linear feedback shift register [14]) складається з двох частин: регістра зсуву і функції зворотного зв'язку. Зсувний регістр – послідовність бітів. Довжина регістру зсуву – кількість бітів. Коли потрібно витягти біт, всі біти регістру зсуву зсуваються вправо на одну позицію. Новий крайній зліва біт визначається функцією інших бітів регістра. На виході регістру зсуву виявляється один, зазвичай молодший, значущий біт. Період регістру зсуву – довжина одержуваної послідовності до початку її повторення.

Для LFSR функція зворотного зв'язку представляє собою суму за модулем 2 (*XOR*) деяких бітів регістра (ці біти називаються відвідної послідовністю). LFSR може перебувати в 2^n–1 внутрішніх станах, де n – довжина регістру зсуву. Якщо зсувний регістр заповнений нулями, то такий стан буде породжувати на виході тільки нулі (так як в якості функції зворотного зв'язку використовується XOR), тому такий стан марно. Теоретично, LFSR може генерувати послідовність довжиною 2^n-1 біт, так як довжина послідовності збігається з кількістю внутрішніх станів. LFSR буде проходити всі внутрішні стани (мати максимальний період) тільки за певних відвідних послідовностях – якщо многочлен, утворений з відвідної послідовності і константи 1, є примітивним за модулем 2. Ступінь многочлена – довжина регістру зсуву, примітивний многочлен ступеня n – це непривідний многочлен, який є дільником $x\ 2^{n-1}+1$, але не є дільником $x\ d + 1$ для всіх d, що поділяють 2^{n-1}.

Наприклад, щоб перевірити чи буде LFSR з відвідною послідовністю, що складається з першого і четвертого бітів, генерувати послідовність максимальної довжини (15 для 4-бітного регістру), потрібно перевірити, чи буде многочлен $x_4 + x + 1$ примітивним [14].

Вихор Мерсенна (Mersenne twister) [20] – це генератор ПВЧ, заснований на властивостях простих чисел Мерсенна і забезпечує швидку генерацію високоякісних псевдовипадкових чисел. Вихор Мерсенна позбавлений багатьох недоліків властивих іншим ГПВЧ, таких як малий період, передбачуваність, легко що виявляється статистична залежність. Тим не менше, цей генератор не є криптостійким, що обмежує його використання в криптографії.

Вихор Мерсенна є витковим регістром зсуву з узагальненою віддачею (twisted generalised feedback shift register, TGFSR). «Вихор» – це перетворення, яке забезпечує рівномірний розподіл генерованих ПВЧ у 623 вимірах (для лінійних конгруентних генераторів воно обмежене 5 вимірами). Тому, кореляція між послідовними значеннями у вихідній послідовності Вихора Мерсенна мала настільки, що нею можна знехтувати [20].

Вихор Мерсенна має величезний період, (доведено, що його період дорівнює числу Мерсенна 2^{19937}-1, що більш ніж достатньо для багатьох практичних застосувань). Існують ефективні реалізації Вихора Мерсенна, що перевершують за швидкістю багато стандартних ГПВЧ (зокрема, в 2-3 рази швидше лінійних конгруентних генераторів). Алгоритм заснований на такому рекурентному виразі [20]:

$$x_{k+n} = x_{k+m} \oplus \left(x_k^u \middle| x_{k+1}^l\right) A, (k = 0,1,\ldots), \qquad (4)$$

де n – ціле, яке позначає ступінь рекурентності, m – ціле, $1<m<n$, A – матриця розміру $W*W$, з елементами з $F2$. У правій частині позначає «старші w-r біт» x_k^u , і x_{k+1}^l, «молодші r біт» x_k+1.

Висновки

Таким чином, у даній роботі виконано дослідження, які відображають ключові аспекти криптографічного захисту ДІР. Зокрема, наведено базові принципи побудови абстрактної моделі порушника в державних ІКС, проаналізовано основні принципи криптографії та проблеми управління ключовими даними в процесі захисту ДІР.

Проведені дослідження дозволяють виділити недоліки існуючих та формалізувати вимоги до побудови нових, більш ефективних, систем криптографічного захисту ДІР.

Література

[1] A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications [Electronic resource]. — Mode of access: World Wide Web. — URL: http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22b.pdf — Descrip-tion based on screen.

[2] Advanced Encryption Standard (AES) [Electronic resource] : FIPS 197. — Electronic data (1 file: 279 457 byte). — Gaithersburg, Maryland, USA : NIST, 2001. — Mode of access: World Wide Web. — URL: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf. — Description based on screen.

[3] Korchenko O. Modern quantum techno-logies of information security against cyber-terrorist attacks / O. Korchenko, Y. Vasiliu, S. Gnatyuk // Aviation. Vilnius : Technika, 2010, Vol. 14, № 2, p. 58–69.

[4] Lai X. Markov ciphers and differential cryptanalysis / X. Lai, J. Massey, S. Murphy // Advances in Cryptology — EUROCRYPT'91, Proceedings. — Springer Verlag, 1991. — P. 17-38.

[5] Lenore Blum, Manuel Blum, and Michael Shub. A Simple Unpredictable Pseudo-Random Number Generator, SIAM Journal on Computing, May 1986, vol. 15, p. 364–383.

[6] Shannon C. Communication Theory of Secrecy Systems, Bell Systems Technical Journal, 1949. — Vol. 28. — P. 656-715.

[7] Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications. NIST Special Publication 800-22, May 15, 2001.

[8] Telecommunications Networks - Current Status and Future Trends / [O. Korchenko, M. Lutskiy,

S. Gnatyuk et al.]; edited by J. H. Ortiz. — Rijeka : InTech, 2012. — 446 p.

[9] Wooters W.K. A single quantum cannot be cloned / W.K. Wooters, W.H. Zurek // Nature. — 1982. — V. 299. — P. 802.

[10] Алексейчук А.Н. Оценки практической стойкости блочного шифра «Калина» относительно методов разностного, линейного криптоанализа и алгебраических атак, основанных на гомоморфизмах / А.Н. Алексейчук, Л.В. Ковальчук, Е.В. Скрынник, А.С. Шевцов // Прикладная радиоэлектроника. — 2008. — Т.7, № 3. — С. 203-209.

[11] Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. // Основы криптографии Учебное пособие. — М.: Гелиос — АРВ, 2005. — 356 с.

[12] Гнатюк С.О. Методика підвищення швидкості криптографічних обчислень / С.О. Гнатюк, В.М. Кінзерявий // «ПОЛІТ–2010. Сучасні проблеми науки»: тези Міжнародної конф. молодих учених і студентів (7–9 квітня 2010 року). – К. : НАУ, 2010. – С. 157–158.

[13] Гнатюк С.О. Систематизація квантових методів криптографічного захисту інформації / С.О. Гнатюк, В.М. Кінзерявий // ПОЛІТ-2010. Сучасні проблеми науки : Міжнародна конференція молодих учених і студентів : тези доповідей. — К. : НАУ, 2010. — С. 153–154.

[14] Горбенко І.Д. Захист інформації в інформаційно-телекомунікаційних системах // І.Д. Горбенко, Т.О. Гріненко. – Х. : 2004. — 222 с.

[15] Горбенко І.Д. Перспективний блоковий симетричний шифр «КАЛИНА». Основні положення та специфікація / І.Д. Горбенко, В.І. Долгов, Р.В. Олійников та ін. // Прикладная радиоэлектроника. — 2007. — Т. 6, № 2. — С. 195-208.

[16] Исагулиев К.П. Справочник по криптологии. М. : Новое знание, 2004. — 237 с.

[17] Кваснiков В.П. Блоковий симетричний криптоалгоритм «LUNA» / В.П. Кваснiков, В.М. Кінзерявий, С.О. Гнатюк, О.М. Кінзерявий // Захист інформації. – №3 (52). – 2011. – С. 77-87

[18] Кінзерявий В.М. Блоковий симетричний алгоритм шифрування / В.М. Кінзерявий, А.В. Марченко, Н.В. Лукашевич, С.О. Гнатюк, О.В. Шевченко // Вісник інженерної академії України. – №1, 2011. – С. 136–140.

[19]Конахович Г.Ф., Шевченко О.В., Кінзерявий В.Н., Хохлачова Ю.Є. Сучасні методи квантової стеганографії // Захист інформації. —2011. — №2 (51). — С. 82-86.

[20] Конкретная математика. Основание информатики // Дональд Кнут, Роналд Грэхем — М. : Мир, 2006. — С. 703.

[21] Корченко О.Г. Систолический криптопроцессор / Корченко О.Г., Гнатюк С.О., Кінзерявий В.М., Панасюк А.Л. // «Інформаційні технології та комп'ютерна інженерія»: тези доповідей Міжнародної наук.-практ. конф. (19–21 травня 2010 року). – Вінниця : ВНТУ, 2010. – С. 187–189.

[22] Корченко О.Г. Спосіб шифрування інформації на основі шифру Файстеля / О.Г. Корченко, Є.В. Паціра, В.М. Кінзерявий, С.О. Гнатюк // Вісник інженерної академії України. – №2, 2009. – С. 117–121.

[23] Корченко О.Г. Швидкодіючий конвеєрний криптографічний обчислювач / О.Г. Корченко, А.Л. Панасюк, С.О. Гнатюк, В.М. Кінзерявий // Вісник Східноукраїнського національного університету імені Володимира Даля – №5 (159), 2011. – С. 317–320.

[24] Корченко О.Г., Луцький М.Г., Гнатюк С.О. Сучасні комерційні системи квантової криптографії // Сучасна спеціальна техніка. – 2011. – №4(27). – С. 37-42.

[25] Корченко О.Г., Скулиш Є.Д., Горбенко Ю.І., Пушкарьов О.І., Соловйов О.А., Коряков І.В. Сучасні системи захисту державних інформаційних ресурсів // Захист інформації. – № 4(53) 2011. – с. 5-17.

[26] Корченко А.Г. Альтернативные средства конфиденциальной связи / А.Г. Корченко, В.А. Рындюк, С.А. Гнатюк, В.Н. Кинзерявый // "Информационные технологии в гуманитарном образовании" им. Т.П. Сарана: III Международная науч.-практ. конф.: сборник статей по материалам докладов конференции – Пятигорск: ПГЛУ, 2010. – С. 357–363.

[27] Корченко О.Г. Імітаційна модель пінг-понг протоколу з парами переплутаних кутритів у квантовому каналі з шумом / О.Г. Корченко, Є.В. Васіліу, С.О. Гнатюк, В.М. Кінзерявий // Захист інформації. – №3, 2010. – С. 46–56.

[28] Корченко О.Г. Імітаційне моделювання роботи системи квантового прямого безпечного зв'язку із застосуванням завадостійких кодів для кутритів / О.Г. Корченко, Є.В. Васіліу, С.О. Гнатюк, В.М. Кінзерявий // Захист інформації. – 2011. – №2 (51). – С. 61–69.

[29] Корченко О.Г. Основні критерії та вимоги до побудови сучасних криптосистем / О.Г. Корченко, С.О. Гнатюк, Ю.Є. Хохлачова, А.О. Охріменко // Вісник інженерної академії України. – №3-4, 2011. – С. 77–83.

[30] Корченко О.Г. Сучасні квантові технології захисту інформації / О.Г. Корченко, Є.В. Васіліу, С.О. Гнатюк // Захист інформації. — 2010. — № 1. — С. 77–89.

[31] Математичні основи криптоаналізу: навч. посібник / С.О.Сушко, Г.В. Кузнецов, Л.Я. Фомичова, А.В. Корабльов. – Д.: Національний гірничий університет, 2010. – 465 с.

[32] Математичні основи криптографії: навч. посібник / Г.В. Кузнецов, В.В. Фомичов, С.О.Сушко, Л.Я. Фомичова. – Д.: Національний гірничий університет, 2004. – Ч.1. – 391 с.

[33] Нильсен М. Квантовые вычисления и квантовая информация / М. Нильсен, И. Чанг. — М. : Мир, 2006. — 824 с.

[34] Панасенко С.П. Алгоритмы шифрования. Специальный справочник. — СПб. : БХВ-Петербург, 2009 — 576 с.

[35] Пат. № 45776 України, МПК H04L 9/06. Спосіб криптографічного перетворення інформації / Корченко О.Г., Паціра Є.В., Кінзерявий В.М., Гнатюк С.О.; заявник та патентовласник Націон. авіаційний ун–тет. – №u200905972; заявл. 10.06.2009; опубл. 25.11.2009, Бюл. №22.

[36] Пат. № 55211 України, МПК H04L 9/06. Конвеєрний криптографічний обчислювач / Корченко О.Г., Паціра Є.В., Панасюк А.Л., Кінзерявий В.М., Гнатюк С.О.; заявник та патентовласник Націон.

авіаційний ун–тет. – № u20100641; Заявл. 19.05.2010; Опубл. 10.12.2010. Бюл. №23. – 8 с.

[37] Пат. № 55213 України, МПК H04L 9/06. Конвеєрний криптографічний обчислювач / Корченко О.Г., Паціра Є.В., Панасюк А.Л., Кінзерявий В.М., Гнатюк С.О.; заявник та патентовласник Націон. авіаційний ун–тет. – № u20100644; Заявл. 19.05.2010; Опубл. 10.12.2010. Бюл. №23. – 8 с.

[38] Положення про проведення відкритого конкурсу криптографічних алгоритмів [Електронний ресурс] // Інститут кібернетики ім. В.М. Глушкова НАНУ; ДСТСЗІ. — Режим доступу: http://www.dstszi.gov.ua/dstszi/control/ru/publish/article;jsessionid=EE63A37FEF8F5B34030F1E38D7247DBC?art_id=48387&cat_id=92733.

[39] Румянцев К.Е. Квантовая криптография : принципы, протоколы, системы / К.Е. Румянцев, Д.М. Голубчиков // Всероссийский конкурс. отбор обзорно-аналитических статей по приоритетному направлению «Информационно-телекоммуникационные системы», 2008. — 37 с.

[40] Физика квантовой информации : Квантовая криптография. Квантовая телепортация. Квантовые вычисления / Ред. Д. Боумейстер [и др.] ; Пер. с англ. С.П. Кулик, Е.А. Шапиро ; Ред. пер. С.П. Кулик, Т.А. Шмаонов. — М. : Постмаркет, 2002. — С. 33–73.

[41] Юдін О.К. Захист інформації в мережах передачі даних : Підручник / О.К. Юдін, О.Г. Корченко, Г.Ф. Конахович. — К. : Видавництво «DIRECTLINE», 2009. — 714 с.

УДК 003.26:004.056.55 (045)

Гнатюк С.А., Кинзерявый В.Н., Охрименко А.О. Особенности криптографической защиты государственных информационных ресурсов

Аннотация. *В статье приведены базовые принципы построения абстрактной модели нарушителя в государственных информационно-комуникационных системах. Рассмотрены основные принципы построения разного рода криптосистем, которые могут использоваться для защиты государственных информационных ресурсов. Кроме этого, проанализировано основные проблемы управления ключевыми данными в процесе защиты государственных информационных ресурсов.*

Ключевые слова: *государственные информационные ресурсы, абстрактная модель нарушителя, криптография, генерация и распределения ключей шифрования, принципы криптографии.*

Gnatyuk S.O., Kinzeryavyy V.M., Okhrimenko A.O. Features of cryptographic protection of state information resources

Abstract. *In this paper the basic principles of abstract model of intruder development in state information and communication systems are given. The main principles of different cryptosystems for state information resources protection are showed. Besides the main problems of keys data management in the process of state information resources protection are analyzed.*

Keywords: *state information resources, abstract model of intruder, cryptography, cryptographic keys generation and distribution, principles of cryptography.*

Отримано *03 лютого 2012 року,* затверджено редколегією *05 червня 2012 року*
(рецензент д.т.н., професор Г.Ф. Конахович)