МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

І.А. Терейковський,
С.О. Гнатюк

ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ

Навчальний посібник

Рекомендовано Методичною радою КПІ ім. Ігоря Сікорського
як навчальний посібник для здобувачів ступеня бакалавра
за освітньою програмою «Системне програмування та спеціалізовані комп'ютерні системи»
спеціальності 123 Комп'ютерна інженерія

Електронне мережне навчальне видання

Київ
КПІ ім. Ігоря Сікорського
2022

Рецензент — Толюпа С. В. доктор технічних наук, професор, професор кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київський національний університет імені Тараса Шевченка

Відповідальний редактор — Тарасенко В.П., доктор технічних наук, професор

Гриф надано Методичною радою КПІ ім. Ігоря Сікорського (протокол № X від DD.MM.YYYY р.) за поданням Вченої ради факультету прикладної математики (протокол № 1 від 01.09.2022 р.)

Навчальний посібник містить основні принципи та технології організації захисту інформації, що циркулює в інформаційно-комунікаційних системах. Висвітлюються базові технології захисту та управління безпекою сучасних інформаційно-комунікаційних систем: міжмережеве екранування, тунелювання, криптографічний захист, безпека бездротових з'єднань, автентифікація, квантовий розподіл ключів та прямий безпечний зв'язок. Орієнтовано для самостійної роботи здобувачів ступеня бакалавр за освітньою програмою «Системне програмування та спеціалізовані комп'ютерні системи» спеціальності 123 «Комп'ютерна інженерія» при вивченні розділу «Основи побудови комплексів засобів захисту в комп'ютерних системах» та розділу «Криптографічні методи і засоби захисту інформації» з дисципліни «Захист інформації в комп'ютерних системах». Також стане у нагоді розробникам програмного забезпечення, аспірантам та студентам технічних снеціальностей.

Реєстр. № НП XX/XX-XXX. Обсяг X,X авт. арк.

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
проспект Перемоги, 37, м. Київ, 03056
https://kpi.ua
Свідоцтво про внесення до Державного реєстру видавців, виготовлювачів і розповсюджувачів видавничої продукції ДК № 5354 від 25.05.2017 р.

Зміст

Список використаних скорочень та абревіатур

БД — база даних;

ВП — випадкова послідовність;

ГВП — генератор випадкових послідовностей;

ГПВП — генератор псевдовипадкових послідовностей;

ГСТУ — Галузевий стандарт України;

ДСТУ — Державний стандарт України;

ІКС — інформаційно-комунікаційна система;

ІТ — інформаційні технології;

КПБЗ — квантовий прямий безпечний зв'язок;

КРК — квантовий розподіл ключів;

НСД — несанкціонований доступ;

ОС — операційна система;

ПВП — псевдовипадкова послідовність;

ПЗ — програмне забезпечення (програмний засіб);

ПК — персональний комп'ютер;

СУБД — система управління базами даних;

СУІБ — система управління інформаційною безпекою;

AES — Advanced Encryption Standard (симетричний алгоритм блочного шифрування, стандарт США);

ARP — Address Resolution Protocol (протокол визначення адрес);

CCMP — Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (протокол блочного шифрування з кодом автентичності повідомлення та режимом зчеплення блоків і лічильника);

CHAP — Challenge Handshake Authentication Protocol (алгоритм автентифікації, що передбачає передачу не безпосередньо пароля, а непрямих відомостей про користувача);

DNS — Domain Name System (система доменних імен);

DSL — Digital Subscriber Line (цифрова абонентська лінія);

DSSS — Direct Sequence Spread Spectrum (розширення спектру методом прямої послідовності);

EAP — Extensible Authentication Protocol (протокол розширеної автентифікації);

FHSS — Frequency Hopping Spectrum Spreading (швидка псевдовипадкова перебудова робочої частоти);

FIN — Final (завершення з'єднання);

FTP — File Transfer Protocol (протокол передачі файлів);

HDLC — High-Level Data Link Control (біт-орієнтований кодопрозорий мережевий протокол управління каналом передачі даних канального рівня моделі OSI).

HTTP — Hyper Text Transfer Protocol (протокол передачі гіпертексту);

HTTPS — Hyper Text Transfer Protocol Secure (протокол передачі гіпертексту безпеки);

ICMP — Internet Control Message Protocol (протокол міжмережевих керуючих повідомлень);

IEC — International Electrotechnical Commission (Міжнародна електротехнічна комісія);

IGMP — Internet Group Management Protocol (протокол управління групами Інтернет);

IKE — Internet Key Exchange (стандартний протокол у складі IPSec для безпечної взаємодії при організації VPN);

IP — Internet Protocol (міжмережевий протокол);

IPSec — Internet Protocol Security VPN (Інтернет протокол безпеки);

IPv4 — Internet Protocol Version 4 (четверта версія IP-протоколу);

IPv6 — Internet Protocol Version 6 (шоста версія IP-протоколу);

IP-адреса — Internet Protocol Address (адреса Інтернет-протоколу);

ISO — International Standartization Organization (Міжнародна організація стандарти-зації);

ITU — International Telecommunication Union (Міжнародний союз електрозв'язку, МСЕ);

L2TP — Layer 2 Tunnelling Protocol (протокол тунелювання другого рівня);

LCP — Link Control Protocol (протокол керування каналом);

MIC — Message Integrity Check (технологія перевірки цілісності повідомлень);

MOSPF — Multicast Open Shortest Path First (мережевий протокол надання найкоротшого шляху);

MPLS — Multi-Protocol Label Switching VPN (багатопротокольна комутація за мітками);

MPPC — Microsoft Point-to-Point Compression (протокол стиснення даних у PPP);

NCP — Network Control Protocols (протокол керування мережею);

NIST — National Institute of Standards and Technology (Національний інститут стандартизації і технологій);

NTLM — NT LAN Manager (диспетчер локальної мережі NT);

OFDM — Ortogonal Frequency Division Multiplexing (метод модуляції з ортогональним частотним мультиплексуванням);

OSI — Open Systems Interconnection (еталонна модель взаємодії відкритих систем);

OSPF — Open Shortest Path First (протокол динамічної маршрутизації);

PAP — Password Authentication Protocol (протокол автентифікації за паролем);

PBCC — Packet Binary Convolutional Coding (метод двійкового пакетного згорткового кодування);

PPP — Point-to-Point Protocol (канальний протокол з'єднання типу «точка-точка»);

PPTP — Point-to-Point Tunneling Protocol (тунельний протокол типу точка-точка);

PSK — Pre-Shared Key (попередньо встановлені ключі);

QoS — Quality of Service (якість обслуговування);

RADIUS — Remote Authentication Dial-In User Service (служба автентифікації віддалених користувачів за комутованими каналами зв'язку);

RIP — Routing Information Protocol (протокол маршрутної інформації);

RPC — Remote Procedure Call (віддалений виклик процедур);

RST — Reset the Connection (обірвання з'єднання);

SA — Security Association (асоціація безпеки в IPSec при організації VPN);

SMTP — Simple Mail Transfer Protocol (простий протокол передачі пошти);

SSL — Secure Sockets Layer (рівень захищених сокетів);

STS — Statistical Test Suite (набір статистичних тестів);

SYN — Synchronize Sequence Numbers (синхронізація номерів послідовності);

TCP / IP — Transmission Control Protocol / Internet Protocol (протокол керування передачею / міжмережевий протокол);

TKIP — Temporal Key Integrity Protocol (протокол інтеграції тимчасового ключа);

UDP — User Datagram Protocol (протокол користувацьких датаграм);

URG — Urgent Pointer Field is Significant (покажчик важливості);

VPN — Virtual Private Network (віртуальна приватна мережа);

WEP — Wired Equivalent Privacy (приватність, еквівалентна дротовим системам);

Wi-Fi — Wireless Fidelity (бездротова точність);

WPA — Wi-Fi Protected Access (захищений доступ Wi-Fi).

Тема 1. Основи захисту інформаційних ресурсів

Базові поняття щодо захисту інформації. Відповідно до законодавства України, під *інформаційно-телекомунікаційною* системою розуміють: 1) сукупність інформаційних (ІС) та телекомунікаційних систем (ТКС), які у процесі оброблення інформації діють як одне ціле; 2) сукупність ІС, мереж і каналів передачі інформації, засобів комунікації і управління інформаційними потоками. Цей термін є вітчизняною адаптацією терміну, прийнятого у світовій практиці, «інформаційно-комунікаційна система» («Information & Communications System»). Фактично, інформаційно-комунікаційна система (ІКС) – це синтез інформаційних (автоматизованих) та комунікаційних (телекомунікаційних) систем (ІС + ТКС).

Під *інформаційною системою,* відповідно до вітчизняного законодавства, розуміють:

1) організаційно-технічну систему, у якій реалізується технологія оброблення інформації з використанням технічних і ПЗ;

2) систему оброблення даних засобами накопичення, зберігання, обновлення та їх пошуку і відображення.

А *телекомунікаційною системою* є сукупність технічних і ПЗ, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

Відповідно, основним призначенням ІКС є забезпечення комунікації (зв'язку) та оброблення *інформації* (відомостей та/або даних, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді).

У типовій ІКС можна виділити такі складові: апаратне забезпечення; ПЗ; інформаційне забезпечення; організаційне забезпечення (сукупність методів і засобів роботи персоналу, який здійснює експлуатацію системи); кадрове забезпечення; правове забезпечення (сукупність норм права, які визначають юридичний статус системи).

Класифікацію ІКС можна проводити за багатьма критеріями – розглянемо найголовніші з них:

1) за *функціональною повнотою* ІКС бувають:

– ІКС для задоволення інформаційних потреб (наприклад, ІС). Такі системи забезпечують доступ користувачів (персоналу, клієнтів) до інформації, її зберігання, пошук тощо;

– ІКС для підтримки бізнес-процесів (так звані інформаційно-аналітичні системи), наприклад, системи підтримки банківських транзакцій.

– ІКС, призначені для управління організаційною структурою (автоматизовані системи управління). Вони повинні забезпечувати автоматизацію комунікацій, документообігу, контролю за виконанням наказів та розпоряджень тощо.

– інтелектуалізовані системи, до яких відносяться експертні системи, системи оцінки ефективності та прогнозування результатів управлінських рішень тощо. Такі системи забезпечують виконання окремих інтелектуальних функцій людини.

2) за *територіальною ознакою:*

– локальні (системи для малого бізнесу);

– середні інтегровані;

– великі інтегровані (глобальні) системи.

3) за *способом організації* ІКС діляться на:

– файл-серверні;

– клієнт-серверні;

– ІКС на базі Інтернет-технологій.

Крім того, з огляду на те, що ІКС фактично поєднує у собі ІС та ТКС, їх можна класифікувати відповідно до відомих класифікацій цих компонентів (наприклад, за способами оброблення інформації в ІС чи за топологією ТКС).

Інформаційні ресурси. Однією з основних складових частин ІКС є інформаційні ресурси. Дані, інформація та знання є абстрактними об’єктами, для роботи з ними необхідна їх матеріалізація у вигляді інформаційних ресурсів. Згідно законодавства України *інформаційний ресурс* – сукупність документів у ІС (бібліотеках, архівах, банках даних тощо).

Документ – це упорядкована сукупність даних, інформації та знань, яка надає можливість доступу, передачі, оброблення тощо. Середовищем зберігання документів є ІКС, яка забезпечує доступ, обмін інформацією та її оброблення. *Інформаційні ресурси* можна класифікувати за такими ознаками:

1. Приналежністю до певної організаційно-технологічної системи (наприклад, бібліотечної мережі, засобів масової інформації, корпоративної системи тощо);

2. Способом виділення об’єктів обліку (твори, документи, видання, бази даних, Інтернет-сторінки тощо);

3. Призначенням ресурсу (масова інформація, освітні ресурси, бізнес-ресурси, особиста переписка тощо)

4. Змістом (за тематичним, об’єктним чи функціональним спрямуванням);

5. Джерелом інформації (національне або закордонне, офіційне або неофіційне джерело тощо);

6. Правовим статусом ресурсу (публічні документи, об’єкти інтелектуальної власності, спам тощо);

7. Структурним типом ресурсу (можливість відділення даних від програм та представлення, формати, кодування тощо);

8. Відкритістю ресурсу (відкритий або з обмеженим доступом);

9. Носієм ресурсу (матеріальний, магнітний тощо);

10. Мовою ресурсу (відповідно до мови створенні чи відображення ресурсу).

Актуальність і важливість проблеми забезпечення безпеки інформаційних ресурсів, обумовлені такими причинами:

– збільшення обчислювальної потужності сучасних ІКС при одночасному спрощенні їх експлуатації та здешевленні;

– різке збільшення обсягів інформаційних потоків даних, що обробляється в ІС та передається каналами ТКС;

– різке зростання кількості розподілених баз даних різного призначення та їх стандартизація й інтеграція до сучасного інформаційного простору;

– високі темпи росту ІТ (інформатизації) у всіх сферах діяльності суспільства (у тому числі й у критичній інфраструктурі держави);

– різке розширення кількості джерел інформації та кола користувачів, які мають безпосередній доступ до інформаційних ресурсів і широкого спектра послуг, що надаються ІС;

– поширення сучасних мережевих технологій серед населення.

Інформаційна безпека ІКС – це стан захищеності ресурсів ІКС, при якому забезпечується їх існування і прогресивний розвиток незалежно від наявності внутрішніх та зовнішніх інформаційних загроз. Іншими словами, під *інформаційною безпекою ІКС* розуміють стан захищеності базових характеристик безпеки інформаційних ресурсів системи, що забезпечує нормальний процес функціонування ІКС та гарантоване надання передбачених послуг системи.

Базовими характеристиками безпеки є конфіденційність, цілісність та доступність *(тріада CIA).*

Конфіденційність – це характеристика безпеки інформації, що відображає її властивість невиявленості й недоступності без відповідних повноважень. Фактично, інформація не може бути доступна або розкрита неавторизованою стороною, тобто для неї її нібито немає.

У свою чергу, легітимна сторона (наприклад, обслуговуючий персонал, користувачі, ПЗ тощо), якій надано відповідні повноваження (легальні атрибути доступу), має повний доступ до інформації.

Цілісність – характеристика безпеки інформації, що відображає її властивість протистояти несанкціонованій модифікації.

Наприклад, користувач, що накопичує інформацію, має право очікувати, що вміст його файлів залишиться незмінним, незважаючи на цілеспрямовані (чи випадкові ненавмисні) впливи, відмови програмних або апаратних засобів. За цією характеристикою інформація не зазнає будь-яких впливів з боку неавторизованої сторони.

Доступність – характеристика безпеки інформації, що відображає її властивість, яка полягає у можливості використання відповідних ресурсів у заданий момент часу відповідно

до пред'явлених повноважень. Фактично, легітимна сторона за потреби, у будь-який момент часу отримує необмежений доступ до потрібної інформації.

Взагалі, ці характеристики можна використовувати для відображення зазначених властивостей цілих ІКС або будь-яких їх компонентів (ПЗ, апаратури, носіїв інформації, даних тощо). Крім зазначених, інколи використовують такі додаткові характеристики безпеки: автентичність, достовірність, безвідмовність (не заперечення авторства) та ін.

Інформаційна безпека є *однією зі сторін розгляду інформаційних відносин* у межах інформаційного законодавства з позицій захисту життєво важливих інтересів особистості, суспільства, держави та акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами. *Об'єктами інформаційної безпеки* є свідомість, психіка людей, ІС та мережі різного масштабу й призначення. До *соціальних об'єктів інформаційної безпеки* зазвичай відносять особистість, колектив, суспільство, державу, світове товариство.

Суб'єкти інформаційної безпеки – держава, що здійснює свої функції через відповідні органи; громадяни; суспільні або інші організації і об'єднання, що володіють повноваженнями щодо забезпечення інформаційної безпеки у відповідності до законодавства.

Інтереси особистості в інформаційній сфері полягають у: реалізації конституційних прав людини та громадянина на доступ до інформації, на використання інформації в інтересах здійснення не забороненої законом діяльності, фізичного, духовного та інтелектуального розвитку; захисті інформації, що забезпечує особисту безпеку тощо.

Інтереси суспільства в інформаційній сфері полягають у:

- забезпеченні інтересів особистості в цій сфері;
- зміцненні демократії;
- створенні правової соціальної держави;
- досягненні та підтриманні суспільного спокою;
- духовному відновленні держави.

Інтереси держави в інформаційній сфері полягають у створенні умов:

- для гармонійного розвитку державної інформаційної інфраструктури;
- для реалізації конституційних прав і свобод людини та громадянина у галузі одержання інформації та користування нею з метою забезпечення непорушності конституційного ладу, суверенітету та територіальної цілісності держави, політичної, економічної та соціальної стабільності, у безумовному забезпеченні законності та правопорядку, розвитку рівноправного та взаємовигідного міжнародного співробітництва.

Інформаційна безпека (у вузькому розумінні) є необхідною, але невід'ємною складовою інших видів безпеки (політичної, економічної, військової, соціальної та інших складових національної безпеки).

Інформаційна безпека (у широкому розумінні) є самостійним видом безпеки поряд з національною, економічною, військовою, соціальною і політичною.

Захист інформації. Також важливим поняттям є *захист інформації,* що, відповідно до законодавства України, визначається як сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї. Іншими словами, *захист інформації* – це комплекс організаційних, правових і технічних заходів для запобігання загрозам інформаційній безпеці й усуненню їх наслідків. Тобто, сутність захисту інформації полягає у виявленні, усуненні або нейтралізації негативних джерел, причин і умов впливу на інформацію.

Ці джерела є загрозою безпеці інформації. У цьому розумінні *захист інформації* ототожнюється з *процесом забезпечення інформаційної безпеки,* як глобальної проблеми безпечного розвитку світової цивілізації, держав, суспільств, окремих громадян тощо.

Серед інших важливих понять варто відзначити:

Безпека інформації – стан інформації, при якому забезпечується збереження усіх її властивостей, визначених обраною (сформованою) політикою безпеки.

Інформаційна зброя – сукупність спеціально організованої інформації та ІТ, що дозволяє цілеспрямовано змінювати (знищувати, спотворювати), копіювати, блокувати інформацію, долати системи захисту, обмежувати доступ законних користувачів, здійснювати дезінформацію, порушувати функціонування носіїв інформації, дезорганізовувати роботу технічних засобів ІКС, що застосовується у ході інформаційної війни (боротьби) для досягнення поставлених цілей.

Інформаційний простір – глобальне інформаційне середовище, яке в реальному масштабі часу забезпечує комплексне оброблення відомостей про протиборчі сторони та їх навколишнє оточення в інтересах підтримки прийняття рішень щодо створення оптимального, для досягнення поставлених цілей, складу сил і засобів та їх ефективного застосування в різних умовах.

Комплексна система захисту інформації – взаємопов’язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації.

Критична інформаційна інфраструктура держави – частина інформаційної інфраструктури, сукупність інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, порушення функціонування яких може призвести до виникнення аварії та/або надзвичайної ситуації, неспроможності держави виконувати свої функції.

Контрольні запитання

1) Поняття ІКС та її складові.

2) Які Ви знаєте базові критерії класифікації ІКС?

3) Що таке «інформаційні ресурси» і яким чином їх можна класифікувати?

4) Що таке «інформаційна безпека ІКС» (у вузькому і широкому розумінні)?

5) Які Ви знаєте базові характеристики захищеності інформації? Дайте їм визначення.

6) У чому полягають інтереси держави, суспільства і громадян в інформаційній сфері?

7) Які є об’єкти і суб’єкти інформаційної безпеки?

8) Поняття «захист інформації», його відмежування від інформаційної безпеки.

9) Дайте визначення поняттям «інформаційний простір» та «комплексна система захисту інформації».

10) Дайте визначення поняттям «інформаційна зброя» та «критична інформаційна інфраструктура держави».

Тема 2. Базові вимоги до організації захисту

Принципи інформаційних відносин та базові вимоги до організації захисту. Основними *принципами інформаційних відносин* є:

- гарантованість права на інформацію;
- відкритість, доступність інформації, свобода обміну інформацією;
- достовірність і повнота інформації;
- свобода вираження поглядів і переконань;
- правомірність одержання, використання, поширення, зберігання та захисту інформації;
- захищеність особи від втручання в її особисте та сімейне життя.

Основні *напрями державної інформаційної політики:*

- забезпечення доступу кожного до інформації;
- забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації;
- створення умов для формування в Україні інформаційного суспільства;
- забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень;
- створення ІС і мереж інформації, розвиток електронного урядування;
- постійне оновлення, збагачення та зберігання національних інформаційних ресурсів;
- забезпечення інформаційної безпеки України;
- сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору.

Згідно з українським законодавством вирішення проблеми інформаційної безпеки має здійснюватися шляхом:

- створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;
- підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань;
- вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності (кіберзлочинності), захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;
- розгортання та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені ІС, в яких обробляється конфіденційна інформація.

Зазвичай, під час *організації захисту ІКС,* висуваються вимоги до таких характеристик:

– способів побудови системи захисту або її окремих компонентів (ПЗ, програмно-апаратного та апаратного забезпечення);

– архітектури ІС (до класу і мінімальної конфігурації робочих станцій, операційного середовища, орієнтації на певну програмну і апаратну платформи, архітектури інтерфейсу);

– застосування певної стратегії захисту;

– витрат ресурсів на забезпечення системи захисту (до обсягів дискової пам'яті для програмної версії і оперативної пам'яті для її резидентної частини, затрат продуктивності обчислювальної системи на вирішення усіх завдань захисту);

– надійності функціонування систем захисту (до кількісних значень показників надійності у всіх режимах функціонування ІС і під час впливу зовнішніх руйнівних чинників, до критеріїв відмов тощо);

– режимів доступу до інформації з обмеженим доступом, що циркулює в ІКС ;

– швидкості обміну інформацією в ІКС, у тому числі з урахуванням використовуваних криптографічних (чи інших) перетворень;

– кількості рівнів повноважень, що підтримуються системою захисту;

– можливості системи обслуговувати певну кількість користувачів;

– тривалості процедури генерації програмної версії системи захисту інформації;

– тривалості процедури підготовки системи захисту до роботи після подачі живлення на компоненти ІКС ;

– можливості системи захисту реагувати на спроби НСД або на інші інциденти;

– наявності і забезпечення автоматизованого робочого місця адміністратора захисту інформації в ІКС;

– складу використовуваного ПЗ, до його сумісності з іншими програмними платформами, до можливості модифікації тощо;

– використовуваних компонентів системи захисту (наявність ліцензії, сертифіката).

Вимоги до компонентів системи захисту ІКС

1) Підсистема управління доступом повинна забезпечувати:

– ідентифікацію, автентифікацію і контроль за доступом користувачів (процесів) до системи, терміналів, вузлів мережі, каналів зв'язку, зовнішніх пристроїв, програм, каталогів, файлів, записів і т.д.;

– управління потоками інформації;

– очищення звільнених ділянок оперативної пам'яті і зовнішніх накопичувачів.

2) Підсистема реєстрації та обліку виконує:

– реєстрацію та облік: доступу в ІС, видачі вихідних документів, запуску програм і процесів, доступу до файлів, що захищаються; передачу даних лініями і каналами зв'язку;

– реєстрацію зміни повноважень доступу, створення об’єктів доступу, що підлягають захисту;

– облік носіїв інформації;

– оповіщення про спроби порушення захисту.

3) Криптографічна підсистема передбачає:

– шифрування конфіденційної інформації (чи інших категорій інформації з обмеженим доступом);

– шифрування інформації, що належить різним суб’єктам доступу (групам суб’єктів), з використанням різних ключів;

– використання атестованих криптографічних засобів захисту інформації.

4) Підсистема забезпечення цілісності здійснює:

– забезпечення цілісності ПЗ та оброблюваної інформації;

– фізичну охорону засобів обчислювальної техніки і носіїв інформації;

– наявність адміністратора (служби) захисту інформації в ІКС;

– періодичне тестування систем захисту та засобів відновлення ІКС;

– використання сертифікованих засобів захисту і ліцензованого ПЗ;

– контроль за цілісністю ПЗ захисту інформації при завантаженні операційного середовищ;

– оперативне відновлення функцій систем захисту після збоїв;

– тестування засобів захисту інформації;

– виявлення і блокування поширення вірусів та іншого шкідливого ПЗ;

– резервне копіювання ПЗ і даних тощо.

Основні принципи організації захисту. При організації ефективного та надійного захисту потрібно керуватися системою принципів. Під *принципами захисту інформації* розуміються основні ідеї і найважливіші рекомендації з питань організації та здійснення робіт для ефективного захисту інформаційних ресурсів. Їх використання дозволяє ефективно організувати роботу щодо захисту інформації. У загальному, принципи захисту інформації можна умовно розділити на дві основні групи: *правові* та *організаційні.*

Правові принципи захисту інформації. Правове регулювання захисту інформації опирається на принципи інформаційного права – вони базуються на положеннях основних конституційних норм, закріплюють інформаційні права і свободи, а також гарантують їх здійснення. Крім того, основні правові засади захисту інформації ґрунтуються на особливостях і юридичних властивостях інформації як повноцінного об’єкту правовідносин. Узагальнено до правових принципів захисту інформації відносяться:

– легітимність (законність);

– пріоритет міжнародного права над внутрішньодержавним;

– економічна доцільність тощо.

Організаційні принципи захисту інформації. Роль організаційного захисту інформації у системі заходів безпеки визначається своєчасністю та правильністю прийнятих управлінських рішень, способів і методів захисту інформації на основі діючих нормативно-методичних документів.

Організаційні методи захисту передбачають проведення *організаційно-технічних* та *організаційно-правових заходів,* а також включають у себе такі принципи захисту інформації:

- науковий підхід до організації захисту інформації;
- планування захисту;
- управління системою захисту;
- безперервність процесу захисту інформації;
- мінімальну достатність засобів захисту;
- системний підхід до організації та проектування систем і методів захисту інформації;
- комплексний підхід до організації захисту інформації;
- відповідність рівня захисту (а також вартості засобів) цінності інформації;
- гнучкість систем захисту;
- багатозональність та багаторубіжність захисту інформації;
- обмеження числа осіб, які мають допуск до захищеної інформації;
- особисту відповідальність персоналу за збереження довіреної їм інформації.

Контрольні запитання

1) Назвіть принципи інформаційних відносин.

2) Напрями державної інформаційної політики.

3) Яким чином має здійснюватися вирішення проблеми інформаційної безпеки згідно з українським законодавством?

4) До яких характеристик мають висуватися вимоги під час організації захисту ІКС? Чому саме до них?

5) До яких підсистем висуваються вимоги при організації захисту інформації, що циркулює в ІКС?

6) Назвіть вимоги до підсистеми управління доступом у складі ІКС.

7) Назвіть вимоги до підсистеми реєстрації та обліку у складі ІКС.

8) Назвіть вимоги до криптографічної підсистеми у складі ІКС.

9) Назвіть вимоги до підсистеми забезпечення цілісності у складі ІКС.

10) Які є правові та організаційні принципи захисту інформації в ІКС?

Тема 3. Загрози та уразливості ІКС

Загрози інформаційним ресурсам ІКС. *Дестабілізуючі чинники інформаційної безпеки* – явища та процеси природного та штучного походження, що породжують інформаційні загрози. *Джерелами дестабілізуючих чинників* можуть бути як окремі особи, так і організації та їх об'єднання. Особливу групу джерел складають ІС і мережі, оскільки вони одночасно є знаряддями приведення в дію інформаційних загроз, каналом їх проникнення у свідомість особистості або суспільну свідомість і генератором випадкових (спонтанних) загроз, що виникають внаслідок технічних несправностей і інших причин. Джерелом дестабілізуючих чинників може бути також природне середовище. Кожному джерелу властиві певні види дестабілізуючих чинників, які можна представити двома групами: міждержавні і внутрішньодержавні дестабілізуючі чинники.

Сукупність джерел разом із властивими їм видами дестабілізуючих чинників формують цілий спектр *інформаційних загроз,* що впливають на стан інформованості особистості, суспільства і держави. До них відносяться: викрадення, знищення, втрата, приховування, спотворення, розголошення, фальсифікація, компрометація критичної інформації, а також фабрикування, розповсюдження і впровадження дезінформації. До *внутрішньодержавних* дестабілізуючих чинників відносять: правовий вакуум у більшості питань забезпечення інформаційної безпеки; навмисне або ненавмисне порушення законодавства з питань інформаційної безпеки; політичні конфлікти; зловмисні дії злочинних елементів або груп; відмови, збої, технічні помилки ІС (засобів); природні явища (процеси), що ускладнюють одержання, передачу, прийом і зберігання інформації або руйнують ІС. *Міждержавні* дестабілізуючі чинники — це конфлікти різноманітних масштабів і проявів у економіці, політиці, ідеології, дипломатії тощо.

Загрози інформаційній безпеці – сукупність умов і чинників, що створюють небезпеку життєво важливим інтересам особистості, суспільства і держави в інформаційній сфері. Основні загрози інформаційній безпеці можна розділити на три групи: 1) Загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації); 2) Загрози несанкціонованого і неправомірного впливу на інформацію та інформаційні ресурси неавторизованих осіб; 3) Загрози інформаційним правам і свободам особистості.

Чинники загроз за видовою ознакою поділяються на політичні, економічні та організаційно-технічні. Під *політичними чинниками загроз* інформаційній безпеці розуміють: а) зміни геополітичної обстановки внаслідок фундаментальних змін у різноманітних регіонах світу; б) інформаційну експансію розвинених країн, які здійснюють глобальний моніторинг світових політичних, економічних, воєнних, екологічних та інших процесів, а також розповсюджують інформацію з метою здобуття односторонніх переваг; в) становлення нової державності у пострадянських країнах на основі принципів демократії, законності,

інформаційної відкритості і, як наслідок, знищення колишньої командно-адміністративної системи державного управління (і відповідно руйнування різного роду систем забезпечення безпеки, порушення інформаційних зв'язків тощо).

Основними *економічними чинниками загроз* безпеці інформації є: a) перехід на ринкові відносини в економіці, поява на ринку великої кількості вітчизняних та зарубіжних комерційних структур (виробників та споживачів інформації, засобів інформатизації та захисту інформації), включення інформаційної продукції у систему товарних відносин; б) критичний стан вітчизняних галузей промисловості, які виробляють засоби інформатизації, комунікації та захисту інформації; в) розширення кооперації із зарубіжними країнами щодо розвитку інформаційної інфраструктури.

Основними *організаційно-технічними чинниками загроз* є: a) недостатня нормативно-правова база у сфері інформаційних відносин, у тому числі в галузі забезпечення інформаційної безпеки; b) недостатнє регулювання державою процесів функціонування та розвитку ринку засобів інформатизації, інформаційних продуктів та послуг; c) широке використання незахищених імпортних технічних та ПЗ для зберігання, оброблення та передавання інформації; d) постійне зростання обсягів інформації, яка передається відкритими каналами ІКС; e) загострення криміногенної обстановки, зростання кількості кіберзлочинів.

Загрози безпеці інформації в ІКС:

- протиправне збирання та використання інформації;
- порушення технології оброблення інформації;
- впровадження в апаратні та ПЗ компонентів, що реалізують функції, не передбачені документацією на ці вироби;
- розробка і поширення програм, що порушують нормальне функціонування компонентів ІКС;
- радіоелектронний вплив з метою виведення з ладу, пошкодження чи руйнування систем оброблення інформації та зв'язку;
- вплив на парольно-ключові системи захисту ІКС;
- впровадження спеціальних електронних пристроїв у технічні засоби оброблення, зберігання та передачі інформації для перехоплення необхідних даних;
- знищення, пошкодження, руйнування чи розкрадання носіїв інформації;
- перехоплення інформації в мережах передачі даних та лініях зв'язку, нав'язування хибної інформації (компрометація);
- порушення законних обмежень на поширення інформації з обмеженим доступом;
- витік інформації технічними каналами.

Технічний канал витоку інформації – сукупність носія інформації, середовища його поширення та засобу технічної розвідки. Виділяють такі технічні канали витоку інформації:

1) Електромагнітний. Причиною його виникнення є електромагнітне поле, пов'язане із проходженням електричного струму в апаратних компонентах ІКС. Електромагнітне поле може індукувати струм у близько розташованих лініях. Цей канал, у свою чергу, має такі складові: радіоканал (високочастотне випромінювання); низькочастотні канали; мережевий канал (наведення на мережу електроживлення); канал заземлення (наведення на проведення заземлення); лінійний канал (наведення на лінії зв'язку між робочими станціями ІКС).

2) Акустичний (віброакустичний). Пов'язаний з поширенням звукових хвиль у повітрі або пружних коливаннях в інших середовищах, що виникають при роботі пристроїв відображення інформації ІКС.

3) Візуальний. Цей канал пов'язаний з можливістю візуального спостереження зловмисником за роботою пристроїв відображення інформації ІКС без проникнення в приміщення, де безпосередньо розташовані компоненти системи. Як засіб одержання інформації у цьому випадку можуть розглядатися фотокамери, відеокамери тощо.

4) Інформаційний. Пов'язаний з доступом до елементів ІКС, до носіїв інформації, до ПЗ (у тому числі до ОС), а також з підключенням до ліній зв'язку. Інформаційний канал може бути розділений на такі складові: канал ліній зв'язку, канал виділених ліній, канал локальних мереж, канал термінальних і периферійних пристроїв тощо.

Модель порушника в ІКС

Абстрактною моделлю порушника (Abstract Model of Intruder) називається формалізований або неформалізований опис можливих дій порушника (ненавмисного чи навмисного), який формується на основі аналізу типу зловмисника, рівня його повноважень, теоретичних знань та практичних навиків. Порушників прийнято поділяти на *зовнішніх* і *внутрішніх.* До внутрішніх належать: 1) співробітники підприємства-власника ІКС; 2) користувачі ІКС, які можуть наносити шкоду інформації як ненавмисно, так і навмисно; 3) технічний персонал, який обслуговує будівлі і приміщення підприємства (електрики, сантехніки, прибиральниці тощо); 4) 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 легітимного облікового запису і згідно системної політики безпеки взагалі не можуть працювати у цій ІКС. Приклад таких порушників: 1) відвідувачі, які можуть завдати шкоди навмисно або через незнання існуючих обмежень; 2) кваліфіковані хакери (спамери, крекери, фрікери тощо); 3) особи, яких найняли конкуренти для отримання необхідних даних; 4) порушники пропускного режиму.

Основною метою порушника є реалізація НСД до інформації, що циркулює в ІКС, з різною ціллю. Виключенням є випадок, коли порушник ненавмисно реалізує НСД – у такому випадку він є *ненавмисним порушником* (не зловмисником). Особливу небезпеку можуть становити порушники, які знаходяться під впливом: кримінальних угрупувань, бізнесових структур, політичних організацій, спецслужб тощо.

Кваліфікація порушника (Intruder`s Qualification) – це сукупність певних знань і вмінь порушника, які він використовує для реалізації НСД до ресурсів ІКС. Можна відзначити кілька типів кваліфікації порушників, що несуть ймовірну загрозу інформації: 1) володіє інформацією щодо функціональних особливостей ІКС взагалі, уміє користуватися штатними засобами; 2) має високий рівень знань і досвід роботи у технічному обслуговуванні аналогічних ІКС; 3) володіє високим рівнем знань у галузі обчислювальної техніки (зокрема, криптографії, теорії алгоритмів та паралельних обчислень) і програмування на мовах розробки ПЗ ІКС чи її аналога; 4) має доступ до глобальних обчислювальних мереж, суперкомп'ютера чи квантового комп'ютера, за допомогою яких може реалізувати потужну атаку на ІКС (наприклад, атаку повного перебору, використовуючи ефективні квантові алгоритми Шора чи Гровера).

Можливості порушника (Intruder`s Ability) щодо впливу на ІКС можна представити у вигляді такої ієрархічної класифікації: 1) має можливість запуску обмеженого набору ПЗ, що реалізує певні функції щодо оброблення даних; 2) може створювати власне ПЗ та модифікувати існуюче, що дозволить створити нові функції оброблення даних; 3) має змогу управляти функціонуванням ІКС, тобто безпосередньо впливати на ПЗ, склад та конфігурацію її технічного забезпечення; 4) має весь обсяг можливостей легітимних користувачів – може розробляти та впроваджувати в експлуатацію технічні засоби ІКС, а також інтегрувати власні технічні засоби з метою подальшого отримання необхідної інформації.

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

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

За характером дій порушників можна класифікувати так:

1) «випадковий порушник» – той, що порушив політику безпеки ІКС (чи певного її сегменту) помилково, ненавмисне і несвідомо у процесі виконання своїх посадових обов'язків чи іншої службової діяльності;

2) «терплячий порушник» – той, що порушив політику безпеки ІКС (чи певного її сегменту) свідомо, навмисно, але без рішучих дій, маскуючись, підбираючи атрибути доступу легальних користувачів з метою подолання засобів управління доступом тощо;

3) «рішучий зловмисник» – той, що має на меті порушити одну із властивостей безпеки інформації, яка циркулює в ІКС. Такий порушник прагне подолати усі існуючі засоби обмеження доступу і отримати можливість безпосереднього доступу до інформації з метою втручання у роботу ІКС, модифікації, знищення чи отримання необхідних даних;

4) «віддалений порушник» – той, що аналізує технічні канали витоку інформації, впливає віддалено за допомогою спеціальних засобів на локальні та розподілені ІКС, включаючи технології VPN, Wi-Fi, WiMAX, LTE тощо.

Для досягнення цілей порушник може використовувати *сукупність релевантних знань, умінь та навиків,* для прикладу: а) досконале знання математичного апарату дозволить йому створити нові методи криптоаналізу і дешифрувати зашифровані дані; б) знання мов програмування (програмної інженерії) дозволить порушнику реалізувати створені методи криптоаналізу, а також модифікувати існуюче ПЗ легітимних користувачів; б) знання методів соціального інжинірингу дозволить порушнику без ґрунтовних знань математики та програмування обійти будь-які системи захисту інформації.

Для більш детальної побудови абстрактної моделі порушника, виходячи з особливостей конкретної ІКС, рекомендується також класифікувати порушників за такими ознаками: *1) за підготовкою до подолання системи фізичного захисту ІКС* (порушник може бути по різному підготовленим до подолання систем фізичного захисту, що може відіграти ключову роль у деяких випадках); *2) за інформованістю про об'єкт атаки* (різний рівень інформованості порушника про особливості ІКС впливатиме на правильність вибору методів та засобів, і, як наслідок, на результат реалізації НСД); *3) за використовуваними методами та засобами* (у залежності від наявного інструментарію порушнику потрібно буде використати певні методи та засоби, що будуть індивідуальними у більшості випадків).

Визначення конкретних характеристик можливих порушників є значною мірою суб'єктивним. Модель порушника, що побудована з урахуванням особливостей конкретної предметної галузі і технології оброблення інформації, може бути подана перерахуванням кількох варіантів його образу. Кожен тип порушника має бути охарактеризований згідно із зазначеними класифікаціями. Усі 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 несанкціоновані дії здійснюються людиною (чи під її керівництвом). Користувачі ІКС є її складовою, необхідним елементом, проте, з іншого боку, вони є основною причиною і рушійною силою порушень. Отже, питання безпеки ІКС, у певній мірі, є питанням людських відносин та людської поведінки.

Уразливості ІКС. Як відомо, ІКС складається з каналів зв'язку, вузлів, серверів, робочих станцій, прикладного і системного ПЗ, баз даних та ін. Всі ці компоненти мають потребу в оцінці ефективності їх захисту. Засоби аналізу захищеності досліджують мережу і

шукають «слабкі» місця в ній, аналізують отримані результати і на їх основі створюють різного роду звіти. У деяких системах замість «ручного» втручання з боку адміністратора знайдена уразливість буде усуватися автоматично (наприклад, у системі System Scanner). Перелічимо деякі з проблем, що ідентифікуються системами аналізу захищеності: лазівки у ПЗ (Back Door) і програми типу «Троянський кінь»; слабкі паролі; сприйнятливість до проникнення з незахищених систем; неправильне налаштування міжмережевих екранів, Web-серверів і баз даних тощо.

Функціонувати такі засоби можуть на мережевому рівні (network-based), рівні ОС (host-based) і рівні ПЗ (application-based). Найбільшого поширення набули засоби аналізу захищеності мережевих сервісів і протоколів. Пов'язано це, в першу чергу, з універсальністю використовуваних протоколів. Вивченість і повсюдне використання таких протоколів, як IP, TCP, HTTP, FTP, SMTP і т.п. дозволяють з високим ступенем ефективності перевіряти захищеність ІС, що працює у цьому мережевому оточенні. Другими за поширеністю є засоби аналізу захищеності ОС. Пов'язано це також з універсальністю і поширеністю деяких ОС (наприклад, UNIX і Windows NT). Однак через те, що кожен виробник вносить в ОС свої зміни (яскравим прикладом є безліч різновидів ОС UNIX), засоби аналізу захищеності ОС аналізують в першу чергу параметри, характерні для всього сімейства однієї ОС. І лише для деяких систем аналізуються специфічні для неї параметри. Засоби аналізу захищеності програм на сьогоднішній день не так багато, як цього хотілося б. Вони поки існують тільки для широко поширених прикладних систем, типу Web-браузери (Netscape Navigator, Microsoft Internet Explorer), СУБД (Microsoft SQL Server, Sybase Adaptive Server) і т.п. Крім виявлення уразливостей, за допомогою засобів аналізу захищеності можна швидко визначити всі вузли корпоративної мережі, доступні у момент проведення тестування, виявити всі використовувані у ній сервіси та протоколи, їх налаштування і можливості для несанкціонованого впливу (як зсередини корпоративної мережі, так і зовні).

Механізми роботи сканерів уразливостей. Існує два основних механізми, за допомогою, яких сканер перевіряє наявність уразливості – *сканування (scan)* і *зондування (probe)*.

Сканування – механізм пасивного аналізу, за допомогою якого сканер намагається визначити наявність уразливості за непрямими ознаками. Цей метод є найбільш швидким і простим для реалізації. У термінах компанії ISS цей метод отримав назву «логічний висновок» (Inference). Згідно компанії Cisco цей процес ідентифікує відкриті порти, знайдені на кожному мережевому пристрої, і збирає пов'язані з портами заголовки (banner), знайдені при скануванні кожного порту. Кожен отриманий заголовок порівнюється з таблицею правил визначення мережевих пристроїв, ОС і потенційних уразливостей. На основі проведеного порівняння робиться висновок про наявність чи відсутність уразливості.

Зондування – механізм активного аналізу, який дозволяє переконатися присутня чи ні на аналізованому вузлі уразливість. Зондування виконується шляхом імітації атаки, що

використовує перевіряєму уразливість. Цей метод більш повільний, ніж «сканування», але майже завжди набагато точніший. У термінах компанії ISS цей метод отримав назву «підтвердження» (Verification). Згідно компанії Cisco цей процес використовує інформацію, отриману в процесі сканування («логічного висновку»), для детального аналізу кожного мережевого пристрою. Цей процес також використовує відомі методи реалізації атак для того, щоб повністю підтвердити передбачувані уразливості і виявити інші уразливості, які не можуть бути виявлені пасивними методами, наприклад схильність до атак типу «відмова в обслуговуванні» («Denial of Service», DoS-атак). На практиці вказані механізми реалізуються такими методами:

1) «Перевірка заголовків» (Banner Check). Зазначений механізм являє собою ряд перевірок типу «сканування» і дозволяє робити висновок про уразливість, спираючись на інформацію в заголовку відповіді на запит сканера. Типовий приклад такої перевірки – аналіз заголовків програми Sendmail або FTP-сервера, що дозволяє дізнатися їх версію і на основі цієї інформації зробити висновок про наявність у них уразливості. Найбільш швидкий і простий для реалізації метод. Однак ефективність перевірок заголовків досить ефемерна. І ось чому. По-перше, Ви можете змінити текст заголовка, завбачливо видаливши з нього номер версії або іншу інформацію, на підставі якої сканер будує свої висновки. І хоча такі випадки рідкісні, нехтувати ними не варто. Особливо у тому випадку, якщо у Вас працюють фахівці у галузі безпеки, які розуміють всю небезпеку заголовків «за замовчуванням». По-друге, найчастіше, версія, що вказується у заголовку відповіді на запит, не завжди говорить про уразливість ПЗ. Особливо це стосується ПЗ, яке розповсюджується разом з початковими текстами (наприклад, у рамках проекту GNU). Ви можете самостійно усунути уразливість шляхом модифікації вихідного тексту, при цьому забувши змінити номер версії в заголовку. І, по-третє, усунення уразливості в одній версії ще не означає, що в наступних версіях ця уразливість відсутня.

2) «Активні зондувальні перевірки» (Active Probing Check). Також відносяться до механізму «сканування». Однак вони засновані не на перевірках версій ПЗ у заголовках, а на порівнянні «цифрового зліпка» (fingerprint) фрагмента ПЗ зі зліпком відомої уразливості. Аналогічним чином діють антивірусні системи, порівнюючи фрагменти сканованого ПЗ з сигнатурами вірусів, що зберігаються у спеціалізованій базі даних. Різновидом цього методу є перевірки контрольних сум або дати сканованого ПЗ, які реалізуються у сканерах, що працюють на рівні ОС. Спеціалізована БД (у термінах компанії Cisco – БД з мережевої безпеки) містить інформацію про уразливість і способи їх використання (атаки). Ці дані доповнюються відомостями про заходи їх усунення. Найчастіше вона використовується і системою аналізу захищеності і системою виявлення атак. Цей метод також досить швидкий, але реалізується важче, ніж «перевірка заголовків».

3) «Перевірка експлойтів» (Exploit Check). Такі перевірки відносяться до механізму «зондування» і засновані на експлуатації різних дефектів у ПЗ. Деякі уразливості не

виявляють себе, поки Ви не «підштовхнете» їх. Для цього проти підозрілого сервісу або вузла запускаються реальні атаки. Перевірки заголовків здійснюють первинний огляд мережі, а метод «Exploit Check», відкидаючи інформацію у заголовках, дозволяє імітувати реальні атаки, тим самим з більшою ефективністю (але меншою швидкістю) виявляючи уразливості на сканованих вузлах. Однак існують випадки, коли імітація атак не завжди може бути реалізована. Такі випадки можна розділити на дві категорії: ситуації, в яких тест призводить до «відмови в обслуговуванні» аналізованого сайту або мережі, і ситуації, при яких уразливість в принципі не придатна для реалізації атаки на мережу.

Як відомо, багато проблем захисту не можуть бути виявлені без блокування або порушення функціонування сервісу або комп'ютера у процесі сканування. У деяких випадках небажано використовувати імітацію атак (наприклад, для аналізу захищеності важливих серверів), тому це може привести до великих витрат (матеріальним і тимчасовим) на відновлення працездатності виведених з ладу елементів корпоративної мережі. У цих випадках бажано застосувати інші перевірки, наприклад, активне зондування або, у крайньому випадку, перевірки заголовків.

Проте, є деякі уразливості (наприклад, перевірка схильності атакам типу «Packet Storm»), які просто не можуть бути протестовані без можливого виведення з ладу сервісу або комп'ютера. У цьому випадку розробники роблять таким чином – за замовчуванням такі перевірки вимкнені і користувач може сам включити їх, якщо бажає. Таким чином, наприклад, реалізовані системи CyberCop Scanner і Internet Scanner. В останній системі такого роду перевірки виділені в окрему категорію DoS. При включенні будь-який з перевірок цієї групи система Internet Scanner видає повідомлення «WARNING: These checks may crash or reboot scanned hosts» («Увага: ці перевірки можуть вивести з ладу або перезавантажити скановані вузли»).

Етапи сканування. Будь-який сканер проводить аналіз у кілька етапів:

1) Збір інформації про мережу. На даному етапі ідентифікуються всі активні пристрої у мережі і визначаються запущені на них сервіси. *2) Виявлення потенційних уразливостей.* Сканер використовує описану вище базу даних для порівняння зібраних даних з відомими уразливостями за допомогою перевірки заголовків або активних зондувальних перевірок. У деяких системах всі уразливості ранжуються за ступенем ризику. Наприклад, у системі NetSonar уразливості діляться на два класи: мережеві та локальні уразливості. Мережеві уразливості (наприклад, впливають на маршрутизатори) вважаються серйознішими у порівнянні з уразливими, характерними тільки для робочих станцій. Аналогічним чином і в Internet Scanner всі уразливості діляться на три ступені ризику: висока (High), середня (Medium) і низька (Low). *3) Підтвердження обраних уразливостей.* Сканер використовує спеціальні методи і моделює (імітує) певні атаки для підтвердження факту наявності уразливостей на обраних вузлах мережі. *4) Генерація звітів.* На основі зібраної інформації система аналізу захищеності створює звіти, що описують виявлені уразливості. Важливим

аспектом є наявність рекомендацій щодо усунення виявлених проблем. І тут по праву лідером є система Internet Scanner, яка для кожної уразливості містить покрокові інструкції для усунення уразливостей, специфічні для кожної ОС. У багатьох випадках звіти також містять посилання на FTP-або Web-сервера, що містять patch'і і hotfix'и, що усувають виявлені уразливості. *5) Автоматичне усунення уразливостей.* Цей етап дуже рідко реалізується у мережевих сканерах, але широко застосовується у системних сканерах. У System Scanner створюється спеціальний сценарій (fix script), який адміністратор може запустити для усунення уразливості. Одночасно зі створенням цього сценарію, створюється і другий сценарій, який скасовує зроблені зміни.

Мережеві компоненти, на які проводяться атаки:

1) Сервери

Сервери призначені для зберігання інформації або надання певних видів послуг. Внаслідок цього, основними класами атак проти серверів є DoS-атаки і спроби розкриття конфіденційної інформації. Специфічними є атаки, які полягають у фальсифікації службових сервісів. Основними завданнями серверів є зберігання та надання доступу до інформації, і деякі види сервісів. Отже, і всі можливі цілі зловмисників можна класифікувати як: отримання доступу до інформації, отримання НСД до послуг, спроба виведення з робочого режиму певного класу послуг, спроба зміни інформації або послуг, як допоміжний етап якоїсь більшої атаки.

Спроби отримання доступу до інформації, що знаходиться на сервері, в принципі нічим не відрізняються від подібних спроб для робочих станцій, і ми розглянемо їх пізніше. Проблема отримання НСД до послуг приймає надзвичайно різноманітні форми і ґрунтується в основному на помилках або недокументованих можливостях самого ПЗ, що надає подібні послуги. А ось проблема виведення з ладу (порушення нормального функціонування) сервісів досить актуальна у сучасному комп'ютерному світі. Клас подібних атак отримав назву DoS – вона може бути реалізована на цілому діапазоні рівнів моделі OSI: фізичному, канальному, мережевому, сеансовому. Зміна інформації або послуг як частина більш великомасштабної атаки є також дуже важливою проблемою в захисті серверів. Якщо на сервері зберігаються паролі користувачів або будь-які дані, які можуть дозволити зловмисникові, змінивши їх, увійти у систему (наприклад, сертифікати ключів), то природно, сама атака на систему почнеться з атаки на подібний сервер. У якості серверів послуг, найбільш часто піддаються модифікації, слід назвати DNS-сервера.

DNS-служба у мережах Intra- і Inter-Net відповідає за зіставлення «вимовних» і легко запам'ятовуються доменних імен (наприклад, www.intel.com або mail.metacom.ru) з їх IP-адресами (наприклад, 165.140.12.200 або 194.186.106.26). Пакети між станціями завжди передаються тільки на підставі IP-адрес, маршрутизатори орієнтуються тільки на їх значення при виборі напрямку відправлення пакета (доменне ім'я взагалі не включається у відправлений пакет), а служба DNS була створена в основному для зручності користувачів

мережі. Як наслідок і в багатьох мережевих ПЗ ім'я віддаленого комп'ютера для більшої гнучкості або для зручності операторів заноситься не у вигляді 4-байтного IP-адреси, а у вигляді доменного імені.

Якщо зловмисникові вдасться дістати права доступу до DNS-сервера, що обслуговує дану ділянку мережі, то він цілком може змінити програму DNS-сервісу. Зазвичай зміна робиться таким чином, щоб за деякими видами запитів замість правильного IP-адреси клієнта видавався IP-адресу будь-якої допоміжної машини зловмисника, а всі інші запити оброблялися коректно. Це дає можливість змінювати шлях проходження трафіку, який можливо містить конфіденційну інформацію, і робити так, що весь потік інформації надходив спочатку прямо в руки зловмисника.

2) Робочі станції

Основною метою атаки на робочу станцію є, звичайно, отримання даних, які обробляються, або локально зберігаються на ній. А основним засобом подібних атак досі залишаються троянські програми. Ці програми за своєю структурою нічим не відрізняються від комп'ютерних вірусів, проте при попаданні на ПК намагаються вести себе як можна непомітніше. При цьому вони дозволяють будь-якій сторонній особі, яка знає протокол роботи з цією троянською програмою, пробляти віддалено з ПК будь-які дії. Тобто основною метою роботи подібних програм є руйнування системи мережевого захисту станції зсередини.

Для боротьби з троянськими програмами використовується як звичайне антивірусне ПЗ, так і кілька специфічних методів, орієнтованих виключно на них. Щодо першого методу, як і з комп'ютерними вірусами, необхідно пам'ятати, що антивірусне ПЗ виявляє величезну кількість вірусів, але тільки таких, які широко розійшлися державою і мали численні прецеденти зараження. У тих же випадках, коли вірус або троянська програма пишеться з метою отримання доступу саме до Вашої ПК або корпоративної мережі, то вона практично з імовірністю 90% не буде виявлена стандартним антивірусним ПЗ. Ті троянські програми, які постійно забезпечують доступ до зараженого ПК, а, отже, тримають на ній відкритий порт будь-якого транспортного протоколу, можна виявляти за допомогою утиліт контролю за мережевими портами. Наприклад, для ОС Microsoft Windows такою утилітою є ПЗ NetStat. Запуск її з ключем «netstat-a» виведе на екран всі активні порти ПК. Від оператора у цьому випадку потрібно знати порти стандартних сервісів, які постійно відкриті на ПК, і тоді, будь-який новий запис на моніторі повинен привернути його увагу. На сьогоднішній день існує вже кілька ПЗ, які виробляють подібний контроль автоматично. Щодо троянських програм, які не тримають постійно відкритих транспортних портів, а просто методично пересилають на сервер зловмисника будь-яку інформацію (наприклад, файли паролів або повну копію тексту, що набирається з клавіатури), можливий тільки мережевий моніторинг. Це досить складне завдання, що вимагає участі кваліфікованого співробітника або громіздкої системи прийняття рішень.

Тому найбільш простий шлях, що надійно захищає як від комп'ютерних вірусів, так і від троянських програм – це встановлення на кожній робочій станції програм контролю за змінами в системних файлах і службових областях даних (реєстрі, завантажувальних областях дисків і т.п.) – так званих адвізоров.

3) Середовище передачі інформації

Природно, основним видом атак на середовище передачі інформації є її прослуховування. Щодо можливості прослуховування всі лінії зв'язку поділяються на: широкомовні з необмеженим доступом; широкомовні з обмеженим доступом; канали «точка-точка». До першої категорії належать схеми передачі інформації, можливість зчитування інформації з яких нічим не контролюється. Такими схемами, наприклад, є інфрачервоні і радіохвильові мережі. До другої та третьої категорій відносяться вже тільки провідні лінії: читання інформації з них можливе або усіма станціями, підключеними до цього дроту (широкомовна категорія), або тільки тими станціями та вузлами комутації через які йде пакет від пункту відправлення до пункту призначення (категорія «точка-точка»).

До широкомовної категорії мереж відносяться мережа TokenRing, мережа EtherNet на коаксіальному проводі та на повторювачах (хабах). Цілеспрямовану (захищену від прослуховування іншими робочими станціями) передачу даних у мережах EtherNet виробляють мережеві комутатори типу свіч (Switch) і різного роду маршрутизатори (роутери). Мережа, побудована за схемою з захистом трафіку від прослуховування суміжними робочими станціями, майже завжди буде коштувати дорожче, ніж широкомовна топологія, але за безпеку потрібно платити.

Щодо прослуховування мережевого трафіку за допомогою підключення зовнішніх пристроїв, існує такий список кабельних з'єднань (за зростанням складності їх прослуховування): *1) невита пара* – сигнал може прослуховуватися на відстані у кілька сантиметрів без безпосереднього контакту; *2) вита пара* – сигнал трохи слабкіше, але прослуховування без безпосереднього контакту також можливо; *3) коаксіальний провід* – центральна жила надійно екранована опліткою: необхідний спеціальний контакт, що розсовує або ріже частину оплітки і проникає до центральної жили; *4) оптичне волокно* – для прослуховування інформації необхідно вклинювання в кабель і дороге устаткування, сам процес приєднання до кабелю супроводжується перериванням зв'язку і може бути виявлений, якщо кабелем постійно передається будь-який контрольний блок даних.

Вивід систем передачі інформації з ладу (DoS-атака) на рівні середовища передачі інформації можливий, але зазвичай він розцінюється вже як зовнішній механічній або електронний (а не програмний) вплив. Можливі фізичне руйнування кабелів, постановка шумів в кабелі і в інфра- та радіо-трактах.

4) Вузли комутації мереж

Атаки на вузли комутації переслідують зазвичай дві мети: або порушення цілісності мережі (DoS-атака), або перенаправлення трафіку за невірним шляхом, що є певним чином вигідним зловмисникові.

Щодо другої мети отримання доступу до таблиці маршрутизації дозволяє змінити шлях потоку можливо конфіденційної інформації в цікаву зловмисника сторону. Подальші його дії можуть бути подібні атаці на DNS-сервер. Досягти цього можна або безпосереднім адмініструванням, якщо зловмисник як-небудь отримав права адміністратора (найчастіше дізнався пароль адміністратора або скористався незміненим паролем за замовчуванням).

Або ж можливий другий шлях атаки з метою зміни таблиці маршрутизації – він заснований на динамічній маршрутизації пакетів, включеній на багатьох вузлах комутації. У такому режимі пристрій визначає найбільш вигідний шлях відправлення конкретного пакету, ґрунтуючись на історії приходу певних службових пакетів мережі – повідомлень маршрутизації (протоколи ARP, RIP та інші). У цьому випадку при фальсифікації за певними законами кількох подібних службових пакетів можна домогтися того, що пристрій почне відправляти пакети шляхом, що цікавить зловмисника, думаючи, що це і є найшвидший шлях до пункту призначення.

При DoS-атаці зловмисник зазвичай змушує вузол комутації або передавати повідомлення невірним «тупиковим» шляхом (як цього можна домогтися ми розглянули вище), або взагалі перестати передавати повідомлення. Для досягнення другої мети зазвичай використовують помилки у ПЗ, запущеному на самому маршрутизаторі, з метою його «зависання». Так, наприклад, зовсім недавно було виявлено, що цілий модельний ряд маршрутизаторів однієї відомої фірми при надходженні на його IP-адресу досить невеликого потоку неправильних пакетів протоколу TCP або перестає передавати всі інші пакети до тих пір, поки атака не припинитися, або взагалі зациклюється.

Сканування діапазону IP-адрес – це одна з перших дій, застосованих хакерами на етапі виявлення інформації. Сканери діапазону діють методом перебору деякої підмножини IP-адрес і подальшого створення звіту за тими вузлами, які на цей момент активні або відповідають на запити PING або ICMP. Отримана інформація може бути використана для побудови карти мережі, на яку націлена атака хакера. Після завершення цієї стадії хакерами звичайно застосовуються методи сканування уразливих портів. Заборона або фільтрація сканування діапазону IP-адрес може запобігти подальші пошуки зловмисниками інформації про уразливі системах.

Найбільш ефективним способом захисту від сканування діапазону IP-адрес є застосування захисних шлюзів, таких як маршрутизатори, брандмауери або розширені proxy-сервери. При прийнятті рішення про захист системи доцільно враховувати особливості роботи Вашого шлюзу, опис його команд та ін. Після прослуховування можна перейти до етапу сканування портів комп’ютера.

Сканування портів (port scaning) – це процес пробного підключення до портів TCP і UDP досліджуваного комп'ютера з метою визначити, які служби на ньому запущені і чи обслуговуються ними відповідні порти, що знаходяться в стані очікування запитів. Визначення таких портів – етап, що має визначальне значення для подальшого з'ясування типу використовуваної ОС, а також працюючих на комп'ютері прикладних програм. Активні служби, які очікують надходження запиту, можуть надати зломщикові можливість отримати важливу інформацію. Зазвичай це відбувається у тому випадку, коли система безпеки комп'ютера не налаштована належним чином або у ПЗ є добре відомі вади у підсистемі захисту.

Типи сканування

TCP-сканування підключенням (TCP connect scan). При такому типі сканування здійснюється спроба підключення за протоколом TCP до цікавого для нас порту з проходженням повної процедури узгодження параметрів (handshake), що складається в обміні повідомленнями SYN, SYN/ACK і ACK. Спроба такого сканування дуже легко виявити. На рис. 1 показана діаграма обміну повідомленнями у процесі узгодження параметрів.

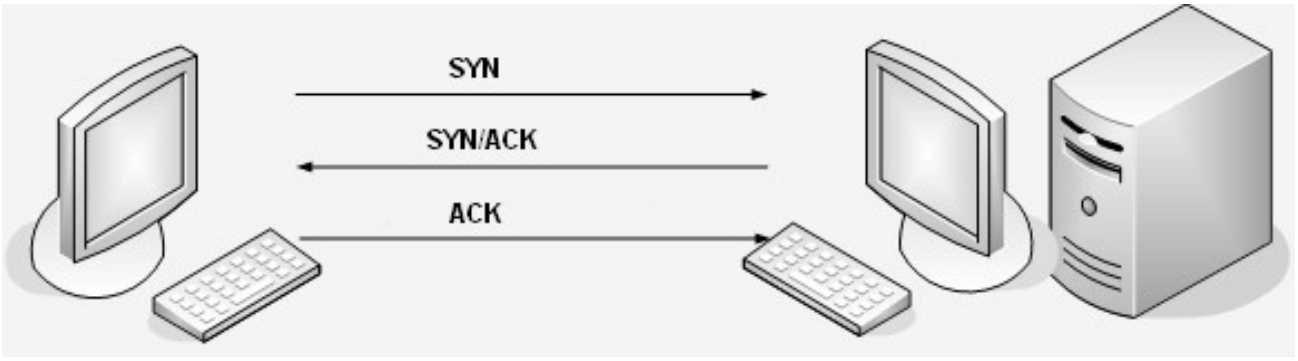

Рис. 1. Схема обміну повідомленнями при встановлені TCP-з'єднання: (1) клієнт відправляє серверу пакет SYN, (2) отримує від сервера пакет SYN/ACK і (3) відправляє серверу пакет ACK

TCP-сканування за допомогою повідомлення SYN (TCP SYN scan). Цей метод називається також сканування з незавершеним відкритим сеансом (half-open scanning), так як при його використанні повне TCP-з'єднання не встановлюється. Замість цього на досліджуваний порт відправляється повідомлення SYN. Якщо у відповідь надходить повідомлення SYN/ACK, це означає, що цей порт знаходиться у стані LISTENG. Якщо ж відповідь приходить у вигляді повідомлення RST/ACK, то, як правило, це говорить про те, що досліджуваний порт відключений. Отримавши відповідь, комп'ютер, що виконує сканування, відправляє до досліджуваного вузла повідомлення RST/ACK, тому повне з'єднання не встановлюється. Цей метод забезпечує більш високу скритність в порівнянні з повним підключенням.

TCP-сканування за допомогою повідомлень FIN (TCP FIN scan). У цьому випадку досліджуваній системі відправляється пакет FIN. Згідно з документом RFC 793, у відповідь

вузол повинен відправити пакет RST для всіх закритих портів. Цей метод спрацьовує лише для стека протоколів TCP/IP, реалізовано у системі UNIX.

TCP-сканування за методом «різдвяної ялинки» (TCP Xmax Tree scan). При використанні цього методу на досліджуваний порт відправляється пакет FIN, URG і PUSH. Згідно з документом RFC 793, досліджуваний вузол у відповідь повинен відправити повідомлення RST для всіх закритих портів.

TCP-нуль-сканування (TCP Null scan). Цей метод полягає у відправці пакетів з відключеними прапорцями. Згідно RFC 793, досліджуваний вузол повинен відповісти відправкою повідомлення RST для всіх закритих портів.

TCP-сканування за допомогою повідомлень ACK (TCP ACK scan). Цей метод дозволяє отримати набір правил, використовуваних брандмауером. Таке сканування допоможе визначити, виконує брандмауер просту фільтрацію пакетів лише певних сполук (пакетів зі встановленим прапором ACK) або забезпечує розширену фільтрацію вхідних пакетів.

TCP-сканування розміру вікна (TCP Windows scan). Такий метод дозволяє виявити відкриті, а також фільтровані порти деяких систем (наприклад, AIX і FreeBSD), залежно від отриманого розміру вікна протоколу TCP.

TCP-сканування порту RPC (TCP RCP scan). Цей метод застосовується тільки для систем UNIX і використовується для виявлення портів RPC (Remote Procedure Call – віддалений виклик процедур), пов'язаних з ними програм і їх версій.

UDP-сканування (UDP scan). Цей метод полягає у відправці на досліджуваний вузол UDP-пакету. Якщо у відповідь надходить повідомлення про те, що порт ICMP недоступний (ICMP port unreachable), це означає, що відповідний порт закритий. Однак якщо такого повідомлення немає, можна припустити, що цей порт відкритий. У зв'язку з тим, що протокол UDP не гарантує доставки, точність такого методу дуже сильно залежить від безлічі факторів, що впливають на використання системних і мережевих ресурсів. Крім того, UDP-сканування – дуже повільний процес, що особливо позначається при спробі сканування пристроїв, у яких реалізований потужний алгоритм фільтрації пакетів.

Виявлення факту сканування. Як правило, зломщики вдаються до сканування TCP- і UDP-портів віддаленого комп'ютера, щоб встановити, які з них знаходяться в стані очікування запитів. Тому виявити факт сканування – означає встановити в якому місці і ким буде зроблено спробу злому. Основні методи виявлення факту сканування полягають у використанні спеціальних програм, призначених для виявлення вторгнення на рівні мережі, таких як snort.

Запобігання скануванню. Навряд чи можна перешкодити будь-кому зробити спробу сканування портів на Вашому комп'ютері, проте цілком реально звести до мінімуму пов'язані з цим ризики. Для цього потрібно заблокувати всі служби, у роботі яких немає необхідності. Однак зробити це, наприклад в ОС Windows, складно, оскільки через мережеву архітектуру системи, принаймні, порти 139 і 443 повинні працювати постійно. Тим

не менш, інші служби можна відключити, запустивши аплет Services панелі управління.

Контрольні запитання

1) Які є загрози та дестабілізуючі чинники безпеці ІКС?

2) Що таке «технічний канал витоку інформації» і які їх види Ви знаєте?

3) Яким чином будується абстрактна модель порушника в ІКС і які характеристики вона зазвичай враховує?

4) За якими критеріями і яким чином можна класифікувати порушників інформаційної безпеки в ІКС?

5) Поняття й функції сканерів уразливостей.

6) Які атаки реалізовує сканер уразливості?

7) На які мережеві компоненти спрямовані атаки сканерів?

8) Які існують механізми та методи роботи сканерів уразливостей?

9) Які етапи сканування виділяють у роботі сканерів уразливостей?

10) Які існують типи сканування портів? Що передує процесу сканування портів?

Тема 4. Технології побудови та функціонування міжмережевих екранів

Особливості застосування міжмережевих екранів. Брандмауер Windows – вбудований в ОС Windows міжмережевий екран, що з'явився у версії Windows XP Sp2. Головною його відмінністю від попередника (яким був Internet Connection Firewall) є контроль доступу програм у мережу. Брандмауер Windows є складовою частиною Центру забезпечення безпеки Windows. За допомогою брандмауера можна запобігти проникненню на комп'ютер хакерів або зловмисних програм (наприклад, мережевих хробаків) через мережу або Інтернет (рис. 2). Крім того, брандмауер запобігатиме надсиланню зловмисних програм із Вашого комп'ютера на інші.

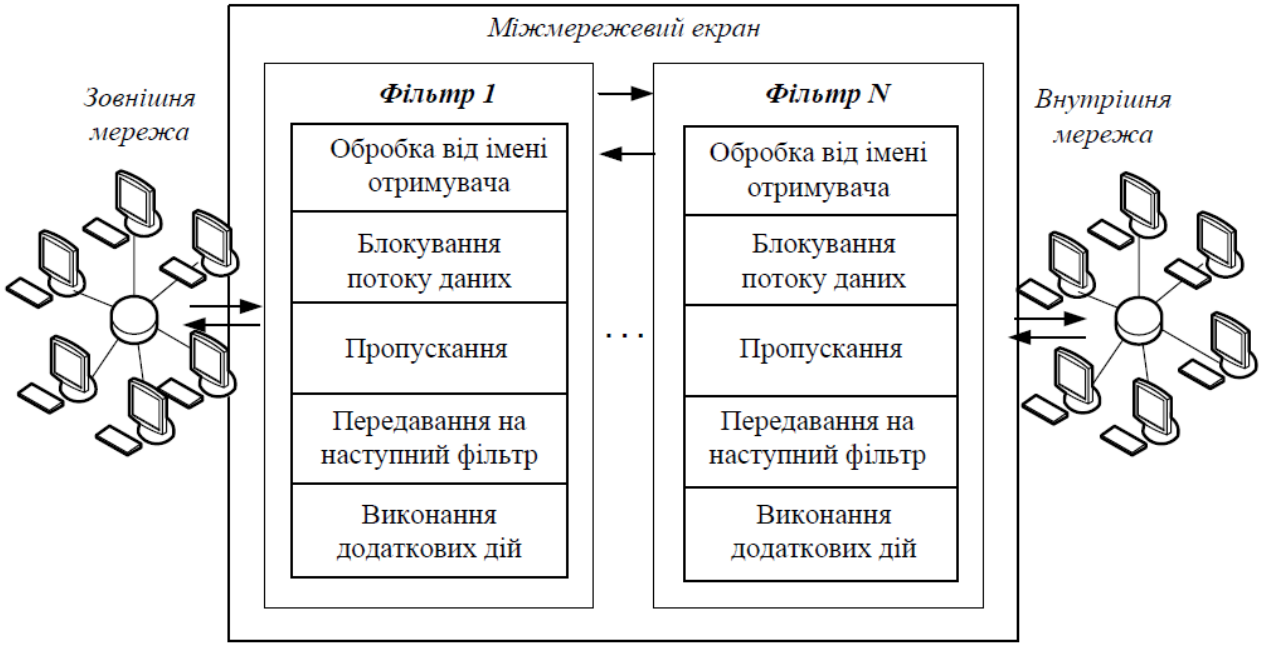

Рис. 2. Логічна структура мережевого екрану

У брандмауер Windows вбудований журнал безпеки, який дозволяє фіксувати IP-адреси та інші дані, що відносяться до з'єднань у домашніх і офісних мережах або в Інтернет. Є можливість запису як успішних підключень, так і пропущених пакетів, що дозволяє відстежувати, коли комп'ютер у мережі підключається, наприклад, до web-сайту (така можливість за замовчуванням відключена, проте її може включити системний адміністратор).

Брандмауер Windows не може запобігти виникненню таких проблем:

– *віруси, які поширюються електронною поштою.* Брандмауер не може визначити вміст електронного повідомлення, тому не захищає від таких типів вірусів. Слід використовувати антивірусну програму для сканування та видалення підозрілих вкладень електронної пошти перед її відкриттям. Навіть якщо на комп'ютері встановлено антивірусну

програму, не слід відкривати вкладення електронної пошти, якщо є сумніви щодо їх безпечності;

– *фішингове шахрайство.* Взагалі, фішинг – це один зі способів ошукання користувачів комп'ютерів з метою отримання приватної або фінансової інформації, наприклад, пароля банківського рахунку. Зазвичай усе розпочинається з повідомлення електронної пошти, яке схоже на повідомлення з надійного джерела, однак насправді воно перенаправляє одержувача на шахрайський web-сайт для збирання особистих відомостей. Брандмауери не можуть визначити вміст електронного повідомлення, тому не захищають від такого роду атак (так званих соціотехнічних атак).

Якщо підключення використовується тільки для доступу до web-ресурсів та електронної пошти, то після включення брандмауер вже готовий до роботи. Однак, якщо на комп'ютері дозволені вхідні або VPN-підключення, то необхідне відповідне налаштування служб. Зрозуміло, що якщо на комп'ютері або у локальній мережі є FTP- або WWW-сервер, то потрібно відзначити ці служби на вкладці Служби (рис. 3), щоб з ними можна було працювати.

Вибравши службу і натиснувши кнопку (Edit), можна потрапити у вікно налаштування її параметрів, де вказується адреса комп'ютера, на якому служба розгорнута, і номери використовуваних портів TCP/IP. При використанні ICMP-запитів слід встановити відповідні прапорці на заданій вкладці (рис. 4).

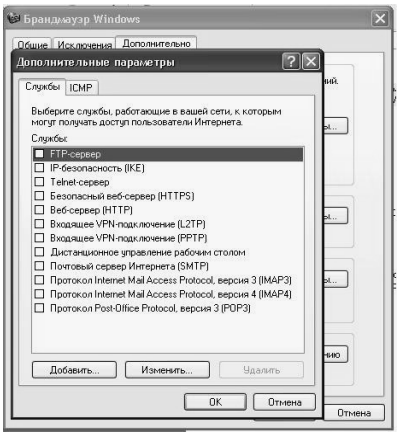

Рис. 3. Вибір дозволених служб, видимих з Інтернет

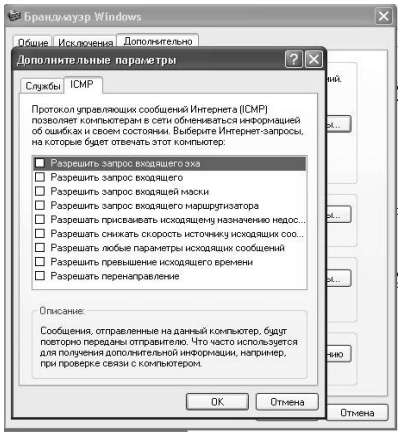

Рис.4. Використання ICMP–запитів

Для того щоб задовольнити вимогам широкого кола користувачів, існує три типи фаєрволів (рис. 5):

- мережевого рівня,
- прикладного рівня,
- рівня з'єднань.

Брандмауери підтримують безпеку міжмережевої взаємодії на різних рівнях еталонної моделі OSI, де функції захисту істотно відрізняються. У зв'язку з цим, комплексний

брандмауер подають у вигляді сукупності неподільних екранів, зорієнтованих на окремий рівень моделі OSI. Зазвичай комплексний екран функціонує на мережевому, сеансовому і прикладному рівнях еталонної моделі, тому відповідно розрізняють екранувальний маршрутизатор та шлюзи сеансового і прикладного рівня (див. рис. 5).

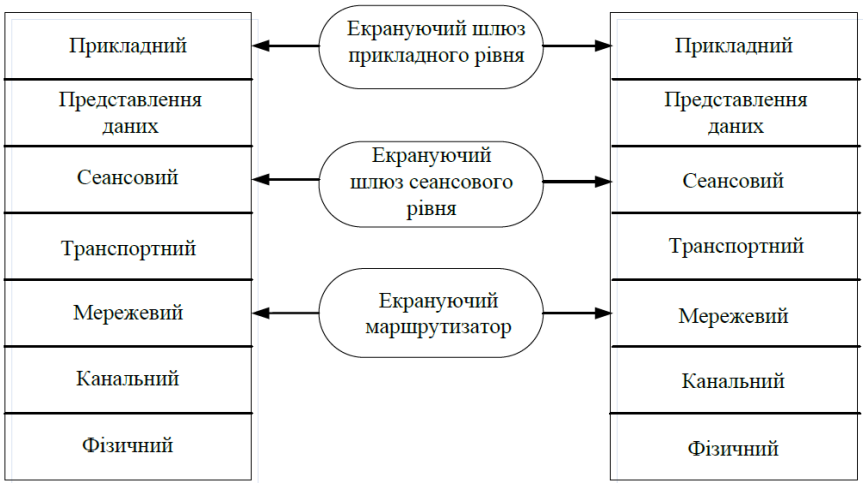

Рис.5. Типи брандмауерів відповідно до моделі OSI

Використовувані в мережах протоколи не завжди однозначно від повідають моделі OSI, і тому зазначені екрани можуть відображати й сусідні рівні еталонної моделі, наприклад, шлюз прикладного рівня може зашифровувати повідомлення при їх передачі та розшифровувати прийняті дані. Тоді він функціонує на рівнях представлення даних і прикладному.

Для міжмережевого екрана окремо задаються правила, які обмежують доступ із внутрішньої мережі в зовнішню, та навпаки. У загальному випадку його робота ґрунтується на динамічному виконанні двох груп функцій:

1) фільтрації інформаційних потоків;

2) посередництва у міжмережевій взаємодії.

При цьому, прості міжмережеві екрани зорієнтовано на виконання тільки однієї із зазначених функцій, а комплексні – забезпечують спільне їх виконання.

Кожен з цих трьох типів брандмауерів використовує свій, відмінний від інших, підхід до захисту мережі:

– ***фаєрвол мережевого рівня*** представлений *екрануючим маршрутизатором*. Він контролює лише дані мережевого і транспортного рівнів службової інформації пакетів. Мінусом таких маршрутизаторів є те, що інші п’ять рівнів залишаються неконтрольованими. Нарешті, адміністратори, які працюють з екрануючими маршрутизаторами, повинні пам’ятати, що у більшості приладів, які здійснюють фільтрацію пакетів *(пакетні фільтри),* відсутні механізми аудиту та подачі сигналу тривоги. Іншими словами, маршрутизатори можуть піддаватися атакам і відбивати велику їх кількість, а адміністратори навіть не будуть

проінформовані. Екрануючі маршрутизатори не забезпечують високого ступеня безпеки, оскільки перевіряють тільки заголовки пакетів і не підтримують таких функцій, як автентифікація кінцевих вузлів, шифрування пакетів, перевірка їх цілісності тощо. Ці маршрутизатори уразливі до таких атак, як підробка вихідних адрес, несанкціонована модифікація вмісту пакетів повідомлень, а обхід таких екранів реалізується на основі формування заголовків пакетів, що задовольняють правилам фільтрації;

– ***фаєрвол прикладного рівня,*** також відомий як *проксі-сервер* (proxy server, сервер-посередник). Фаєрволи прикладного рівня встановлюють певний фізичний поділ між локальною мережею та Інтернет, тому вони мають відповідати найвищим вимогам безпеки. Проте, оскільки ПЗ повинен аналізувати пакети і приймати рішення щодо контролю доступу до них, фаєрволи прикладного рівня неминуче зменшують продуктивність мережі, з огляду на це у якості сервера-посередника необхідно використовувати більш швидкі комп'ютери. Функціонує на прикладному рівні моделі OSI, охоплюючи також рівень представлення даних, забезпечує найбільш надійний захист міжмережевих взаємодій. Його захисні функції належать до функцій посередництва, але, на відміну від шлюзу сеансового рівня, він виконує більшу кількість функцій захисту, до яких належать ті, що реалізуються екранувальними агентами і використовуються по одному для кожного обслуговуваного прикладного протоколу. Прикладний шлюз, аналогічно шлюзу сеансового рівня, перехоплює за допомогою відповідних агентів вхідні і вихідні пакети, копіює та перенаправляє інформацію через шлюз, функціонуючи як сервер-посередник (крім прямих з'єднань між внутрішньою і зовнішньою мережами). Посередники, що використовуються прикладним шлюзом, мають важливі відмінності від канальних посередників шлюзів сеансового рівня, так як вони пов'язані з конкретними прикладними програмами, а також вони можуть фільтрувати потік повідомлень на прикладному рівні моделі OSI. Як і у випадку шлюзу сеансового рівня, для зв'язку між комп'ютерами внутрішньої і зовнішньої мережі відповідний посередник прикладного шлюзу утворює два з'єднання: від комп'ютерів (внутрішньої мережі) до брандмауера і від брандмауера до місця призначення. Але, на відміну від канальних посередників, посередники прикладного шлюзу пропускають лише пакети, згенеровані тими прикладними програмами, які їм доручено обслуговувати. Основними недоліками такого фаєрволу є велика ресурсоємність, складність інсталювання та конфігурування.

– ***фаєрвол рівня з'єднань (сеансового рівня)*** схожий на фаєрвол прикладного рівня тим, що обидва є серверами-посередниками. Відмінність полягає у тому, що фаєрволи прикладного рівня вимагають спеціального ПЗ для кожної мережевої служби (на зразок FTP або HTTP). Натомість, фаєрволи рівня з'єднання обслуговують велику кількість протоколів. Однак, якщо пакетний фільтр при аналізі заголовків перевіряє тільки номери портів джерела й одержувача, то екранувальний шлюз сеансового рівня аналізує інші поля, що стосуються процесу квотування зв'язку (контроль за установленням віртуального з'єднання між вузлами внутрішньої і зовнішньої мережі за допомогою канальних посередників). Здебільшого

екранувальні шлюзи сеансового рівня працюють у комплекті з екранувальними шлюзами прикладного рівня, доповнюючи їх функціями контролю віртуальних з'єднань і трансляції внутрішніх адрес (наприклад, IP-адрес).

Для ефективного захисту міжмережевої взаємодії брандмауер має бути правильно встановлений і налаштований. Для цього необхідно:

1) розробити політику міжмережевої взаємодії;

2) визначити схеми підключення міжмережевого екрана;

3) налагодити параметри функціонування брандмауера.

У табл. 1. міститься *рейтинг брандмауерів* (за результатами незалежного тестування у рамках проекту matousec.com**).** Можна відмітити беззмінне лідерство безкоштовного продукту Comodo Internet Security Premium. Традиційно дуже хороший захист забезпечує фаєрвол, що входить до складу Kaspersky Internet Security. І досить несподівано проявив себе у світлі сучасних загроз мережевий екран (який вважався одним із найперспективніших), включений у BitDefender Total Security, що отримав незадовільну оцінку.

Таблиця 1

Статистика ефективності брандмауерів

Продукт	**Захист**	**Рівень захисту**
1	*2*	*3*
Comodo Internet Security Premium 6.0.260739.2674FREE	92,00%	Відмінний
Privatefirewall 7.0.28.1FREE	88,00%	Дуже хороший
Kaspersky Internet Security 2013 13.0.1.4190	86,00%	Дуже хороший
Outpost Security Suite Pro 7.5.2.3939.602.1809	86,00%	Дуже хороший
SpyShelter Firewall 1.5	79,00%	Хороший
Outpost Security Suite Free 7.1.1.3431.520.1248FREE	71,00%	Хороший
VirusBuster Internet Security Suite 4.1	71,00%	Хороший
Jetico Personal Firewall 2.1.0.10.2451	59,00%	Слабкий
ESET Smart Security 5.2.9.1	51,00%	Слабкий
ZoneAlarm Extreme Security 2013 11.0.000.038	34,00%	Дуже слабкий
ZoneAlarm Free Antivirus + Firewall 11.0.000.020FREE	34,00%	Дуже слабкий
Total Defense Internet Security Suite 8.0.0.87	21,00%	Незадовільний
avast! Internet Security 7.0.1456	15,00%	Незадовільний
Dr.Web Security Space 8.0.0.12060	11,00%	Незадовільний
Webroot SecureAnywhere Complete 2013 8.0.2.66	11,00%	Незадовільний
Avira Internet Security 2013 13.0.0.2693	9,00%	Незадовільний
Bitdefender Total Security 2013 16.18.0.1406	9,00%	Незадовільний

Таблиця 1 (продовження)

1	*2*	*3*
Norton Internet Security 2013 20.2.0.19	9,00%	Незадовільний
TrustPort Total Protection 2013 13.0.3.5073	8,00%	Незадовільний
PC Tools Internet Security 2012 9.1.0.2898	6,00%	Незадовільний
eScan Internet Security Suite 11.0.1139.1150	5,00%	Незадовільний
FortKnox Personal Firewall 8.0.205.0	5,00%	Незадовільний
ThreatFire 4.7.0.53FREE	5,00%	Незадовільний
ArcaVir Internet Security 2012 12.8.6401.1	4,00%	Незадовільний
G Data TotalSecurity 2013 23.0.4.0	4,00%	Незадовільний
Norman Security Suite PRO 10.00	4,00%	Незадовільний

Для розв'язання різноманітних задач в ОС Ubuntu є можливість встановлювати додаткові програми за рахунок пакетів, які завантажуються з репозиторіїв (Repository) в Інтернет. Для того, щоб завантажити та встановити необхідний пакет, необхідно виконати команду *apt-get install.*

Синтаксис команди:

apt-get install […назва пакету…]

Для виконання цієї команди необхідні права адміністратора, тому її потрібно використовувати з параметром sudo. Також, під час встановлення інколи є необхідною участь користувача, який підтвердить встановлення чи здійснить вибір каталогу для встановлення. Приклад команди:

sudo apt-get install dkms

Політика міжмережевої взаємодії. Політика міжмережевої взаємодії є тією частиною політики безпеки в організації, яка визначає вимоги до безпеки інформаційного обміну із зовнішнім світом. Ці вимоги обов'язково повинні відображати два ключові аспекти: 1) політику доступу до мережевих сервісів; 2) політику роботи брандмауера.

Політика доступу до мережевих сервісів визначає правила надання, а також використання, усіх можливих сервісів захисту комп'ютерної мережі. Відповідно, у рамках цієї політики повинні бути задані всі сервіси, що надаються через мережевий екран, допустимі адреси, клієнтів для кожного сервісу. Крім того, повинні бути вказані права для користувачів, що описують коли і які користувачі, яким конкретно сервісом і на якому комп'ютері можуть скористатися. Окремо визначають правила автентифікації користувачів і комп'ютерів, а також умови роботи користувачів поза локальною мережею організації.

Політика роботи брандмауера задає базовий принцип управління міжмережевою взаємодією, що покладений в основу функціонування брандмауера. Необхідно обрати один з двох ключових принципів:

– заборонено все, що не дозволено;

– дозволено все, що не заборонено.

Залежно від вибору, рішення може бути ухвалене як на користь безпеки і на шкоду зручності використання мережевих сервісів, так і навпаки У першому випадку міжмережевий екран повинен бути налаштований таким чином, щоб блокувати будь-які явно не дозволені між мережеві взаємодії. Враховуючи, що такий підхід дозволяє адекватно реалізувати принцип мінімізації привілеїв, він, з точки зору безпеки, є кращим. Тут адміністратор не зможе через забудькуватість залишити дозволеними будь-які повноваження, так як за замовчуванням вони будуть заборонені. Наявні зайві сервіси можуть бути використані на шкоду безпеки, що особливо характерно для закритого і складного ПЗ, у якому можуть бути різні помилки і некоректність. Принцип «заборонено все, що не дозволено», по суті є визнанням факту, що незнання може заподіяти шкоду.

При виборі принципу «дозволено все, що не заборонено» міжмережевий екран налаштовується таким чином, щоб блокувати тільки явно заборонені міжмережеві взаємодії. У цьому випадку підвищується зручність використання мережевих сервісів з боку користувачів, але знижується безпека міжмережевої взаємодії. Адміністратор може врахувати і всі дії, які заборонені користувачам, таким чином йому доводиться працювати у режимі реагування, передбачаючи і забороняючи ті міжмережеві взаємодії, які негативно впливають на безпеку мережі.

Контрольні запитання

1) Що таке «брандмауер» («фаєрвол») і з яких компонентів складається?

2) Які існують типи фаєрволів?

3) Що таке «політика міжмережевої взаємодії»? Які вона має компоненти?

4) Яке необхідне додаткове ПЗ для налаштування фаєрволу в ОС Ubuntu?

5) Які основні відмінності у налаштуванні роботи фаєрволів у ОС Windows та Ubuntu?

6) Реалізації яких загроз типовий фаєрвол не зможе запобігти?

7) Охарактеризуйте роботу брандмауерів з інтерпретацією на модель OSI.

8) У чому полягають основні переваги та недоліки проксі-сервера?

9) Опишіть логічну структуру типового мережевого екрану.

10) Які кроки необхідно виконати для забезпечення ефективного захисту міжмережевої взаємодії?

Тема 5. Принципи побудови віртуальних приватних мереж

Базові принципи побудови віртуальних приватних мереж. *Віртуальна мережа (Virtual Network)* – це виділена мережа на базі загальнодоступної мережі, що підтримує конфіденційність переданої інформації за рахунок використання тунелювання (tunneling) та інших процедур захисту. У основі технології VPN (Virtual Private Network) лежить ідея забезпечення доступу віддалених користувачів (Remote Access Users) до корпоративних мереж, що містять конфіденційну інформацію, через мережі загального користування (рис. 1.5.1).

Порівнюючи приватні і віртуальні приватні мережі, слід виділити безсумнівні переваги VPN:

– технологія VPN дозволяє значно знизити витрати щодо підтримки працездатності мережі: користувач платить тільки абонентську плату за оренду каналу. До речі, оренда каналів також не викликає будь-яких проблем внаслідок широкомасштабності мережі Інтернет;

– така технологія є зручною і легкою при організації, а також перебудові (модифікації) структури мережі.

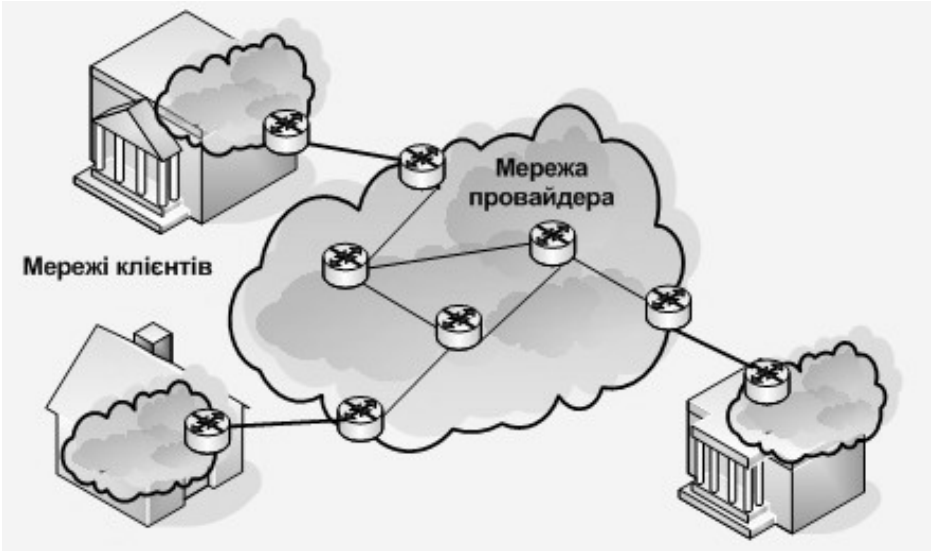

Рис. 6. Загальна схема організації VPN мережі

Розробка єдиної моделі обслуговування VPN мереж могла б спростити мережеві операції, але такий підхід не може задовольнити різним вимогам клієнтів, так як вони є унікальними та непередбачуваними. Кожен клієнт пред'являє свої вимоги до інформаційної безпеки, числа сайтів, складності маршрутизації, критичних застосунків, моделей і обсягів трафіку. Усі мережі VPN *за призначенням* умовно можна розділити на такі основні види:

– *Внутрішньокорпоративні VPN (Intranet VPN).* Інтрамережа – це найбільш простий варіант VPN, що дозволяє об'єднати в єдину захищену мережу кілька розподілених філій

однієї організації, що взаємодіють відкритими каналами зв'язку (такий варіант мережі інколи називають «точка-точка»);

– *Міжкорпоративні VPN (Extranet VPN).* Екстрамережі – варіант побудови VPN «екстра мережі», призначений для забезпечення доступу з мережі однієї компанії до ресурсів мережі іншої, рівень довіри до якої набагато нижче, ніж до своїх співробітників. Тому, коли кілька компаній приймають рішення працювати разом і відкривають один для одного свої мережі, вони повинні подбати про те, щоб їх нові партнери мали доступ тільки до певної інформації;

– *VPN із віддаленим доступом (Remote Access VPN).* Використовують для створення захищеного каналу між сегментом корпоративної мережі (центральним офісом або філією) і одиночним користувачем, який, працюючи вдома, підключається до корпоративних ресурсів з домашнього комп'ютера, корпоративного ноутбука чи смартфона;

– *Інтернет VPN (Internet VPN).* Використовується для надання доступу до Інтернет провайдерами, у випадку якщо через однин фізичний канал підключаються декілька користувачів;

– *Клієнт/сервер VPN (Client / Server VPN).* Цей тип VPN забезпечує захист переданих даних між двома вузлами (не мережами) корпоративної мережі. Особливість цього варіанту у тому, що VPN будується між вузлами, що перебувають, як правило, в одному сегменті мережі, наприклад, між робочою станцією і сервером. Така необхідність часто виникає у тих випадках, коли в одній фізичній мережі необхідно створити декілька логічних мереж. Наприклад, коли треба розділити трафік між фінансовим департаментом та відділом кадрів, що звертаються до серверів, які знаходяться в одному фізичному сегменті.

За *способом реалізації* віртуальні приватні мережі можна розділити так:

– *VPN у вигляді спеціального програмно-апаратного забезпечення.* Реалізація такої мережі здійснюється за допомогою спеціального комплексу програмно-апаратних засобів, забезпечує високу продуктивність і, як правило, високий ступінь захищеності;

– *VPN у вигляді програмного рішення.* Використовують робочу станцію зі спеціальним програмним забезпеченням, що забезпечує функціональність VPN;

– *Інтегроване рішення* – функціональність VPN забезпечує комплекс, що розв'язує також задачі фільтрації мережевого трафіка, організації мережевого екрана й забезпечення якості обслуговування.

Серед сучасних технологій побудови VPN можна назвати такі: Internet Protocol Security (IPSec) VPN, Multi-protocol label switching (MPLS) VPN, VPN на основі технологій тунелювання PPTP (Point-to-Point Tunneling Protocol) і L2TP (Layer 2 Tunnelling Protocol). У всіх перерахованих випадках трафік надсилається у мережу провайдера за протоколом IP, що дозволяє провайдеру надавати не тільки послуги VPN, але і різні додаткові сервіси (контроль за роботою клієнтської мережі, хостинг Web і поштових служб, хостинг спеціалізованих застосунків клієнтів тощо).

Технології VPN поділяються:

1) VPN на базі орендованих каналів. Територіальні канали, що орендуються, прокладаються провайдером транспортних територіальних послуг в його первинній мережі FDM (Frequency Division Multiplexing – технологія частотного мультиплексування), PDH (Plesiochronous Digital Hierarchy – плезіохронна цифрова ієрархія), SDH (Synchronous Digital Hierarchy – синхронна цифрова ієрархія) або мережі з інтегральними послугами ISDN (Integrated Services Digital Network – цифрова мережа з інтеграцією служб). За умов оренди каналу, у таких мережах підприємство ділить пропускну спроможність магістральних каналів і комутаторів цієї мережі з іншими абонентами цього провайдера. Канали, що зв'язують центральну мережу підприємства з мережами філій, проходять через мультиплексор, об'єднуючий канали всіх абонентів у магістральний канал. Не дивлячись на те, що територіальні канали, в цьому випадку, вже не відносяться до власності підприємства, корпоративні мережі, побудовані на орендованих каналах, також називають приватними, з двох причин. По-перше, смуга пропускання орендованого каналу повністю виділяється підприємству, і тому є в деякому розумінні його «приватною власністю». Це повною мірою відноситься до орендованих цифрових каналів, які підтримуються провайдером на базі первинної цифрової мережі з технологією мультиплексування TDM (Time Division Multiplexing – мультиплексування з розділенням часу). Наявність гарантованої пропускної спроможності дає можливість адміністраторові мережі планувати роботу застосунків через глобальні канали зв'язку: розподіляти пропускну спроможність каналу між застосунками, оцінювати можливі затримки повідомлень, обмежувати об'єм територіального трафіку, що генерується, визначати максимальну кількість активних застосувань. По-друге, приватний характер мереж, побудованих на орендованих каналах, підтверджується достатньою конфіденційністю даних. Корпоративні дані практично не доступні для абонентів, що не є користувачами корпоративної мережі або співробітниками організації-провайдера каналів. Комутацію каналів у первинних мережах може виконати лише оператор мережі – це забезпечує великий ступінь захищеності даних, що передаються каналами первинних мереж. Таки чином, забезпечується прийнятна безпека даних, що передаються, без використання шифрування і взаємної автентифікації абонентів. Мережа, побудована на орендованих каналах, володіє такими перевагами: гарантована пропускна спроможність, високий ступінь безпеки, ізольованість адресних просторів. Але цій мережі властиві і недоліки: висока вартість, складна масштабованість тощо;

2) VPN на базі мережі зі встановленням віртуальних каналів – ATM (Asynchronous Transfer Mode), FR (Frame Relay). У цьому випадку віртуальні канали імітують сервіс виділених каналів (гарантована пропускна спроможність, ізоляція трафіку). Послуга реалізується можливостями 2-го рівня моделі OSI, трафік у такій мережі не шифрується;

3) VPN на базі MPLS. Технологія MPLS дозволяє пересилати дані за допомогою міток, що прикріплюються до кожного пакету. Внутрішні вузли ядра мережі не потребують аналізу

вмісту кожного пакету. Зокрема, не розглядається IP-адреса одержувача, що дає можливість MPLS надати ефективний механізм інкапсуляції для приватного трафіку, передаваного магістраллю сервіс-провайдера. Мережа MPLS може розділяти трафік і забезпечувати його захист без шифрування і тунелювання. Технологія MPLS підтримує безпеку у кожній окремій мережі, так само, як і мережі Frame Relay та ATM підтримують її для кожного окремого з'єднання. Якщо традиційна мережа VPN надає базові послуги мережевого транспорту, то мережа з технологією MPLS – це масштабовані послуги VPN, що допускають підтримку IP-застосунків з доданою цінністю поверх базової транспортної мережі VPN. MPLS-VPN – це справжня однорангова VPN, яка розділяє трафік на 3-му рівні моделі OSI за допомогою роздільних IP VPN таблиць передачі. MPLS-VPN може відокремити трафік одного замовника від іншого, тому що кожній мережі VPN кожного замовника привласнюється унікальний ідентифікатор. Це створює такі ж умови безпеки, як в мережах ATM і Frame Relay, тому що користувач мережі VPN не може бачити трафік, що передається за межами цієї мережі;

4) VPN на базі публічної IP-мережі з використанням протоколу IPSec. Протокол IPSec пропонує методи шифрування мережевого рівня, що забезпечує можливість автентифікації і сервіс шифрування між кінцевими точками у загальнодоступних IP-мережах.

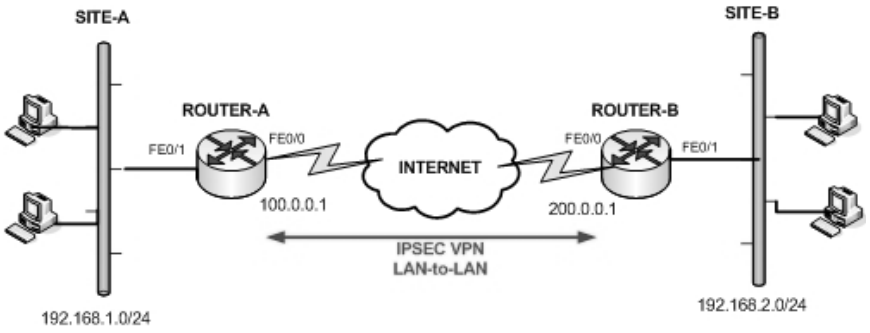

Рис. 7. Побудова захищеного ізольованого тунелю за протоколом IPSec

IPSec VPN. Протокол відноситься до найбільш поширених і популярних у технології VPN, він забезпечує високий ступінь гнучкості, дозволяючи вибирати потрібний режим захисту, а також дозволяє використовувати різні алгоритми автентифікації і шифрування даних. Режим інкапсуляції пакетів дає можливість ізолювати адресні простори клієнта і провайдера за рахунок застосування двох IP адрес – зовнішньої і внутрішньої. IPSec, як правило, застосовується для створення VPN, підтримуваних провайдером, тунелі в них будуються на базі пристроїв клієнта, але конфігуруються вони віддалено і управляються провайдером. Технологія IPSec дозволяє розв'язувати такі задачі щодо встановлення і підтримання захищеного каналу: автентифікацію користувачів або комп'ютерів при ініціалізації каналу; шифрування і автентифікацію переданих даних між кінцевими точками

каналу; автоматичне постачання точок секретними ключами, необхідними для роботи протоколів автентифікації і шифрування даних.

IPSec опирається на ряд технологічних рішень і методів шифрування, але його дію у загальному можна представити у вигляді таких кроків (рис. 8):

1) Потік трафіку. Тип трафіку, який повинен захищатися засобами IPSec, визначається у рамках політики захисту для VPN. Потім ця політика реалізується у вигляді команд конфігурації інтерфейсів пристроїв кожної сторони IPSec. Для визначення трафіку, який потрібно шифрувати, використовують списки доступу, які реалізують політику шифрування. Коли трафік, що підлягає шифруванню, генерується клієнтом IPSec або проходити через нього, клієнт ініціює наступний крок процесу, починаючи першу фазу *IKE.*

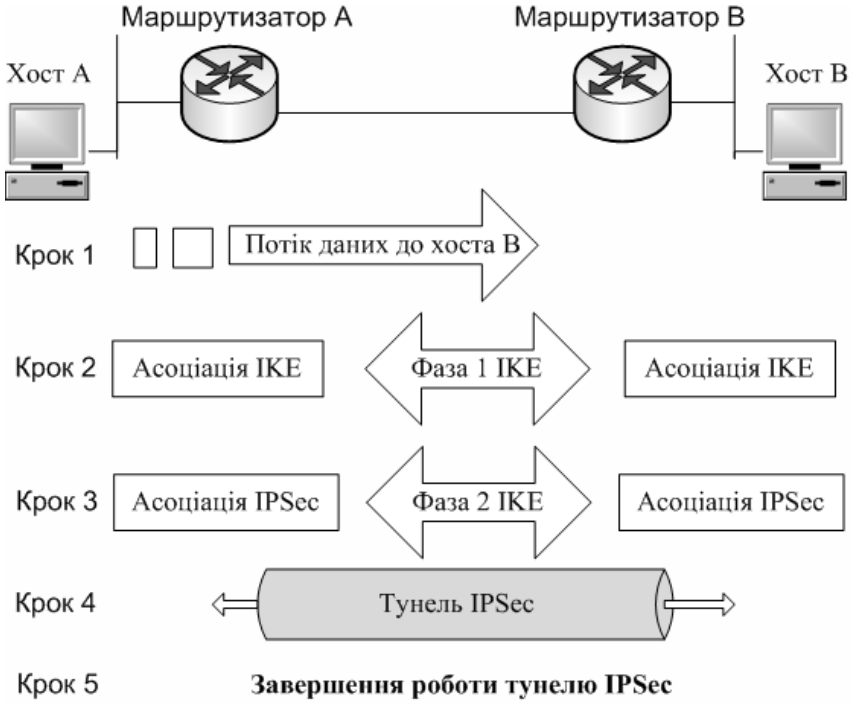

Рис. 8. П’ять кроків роботи протоколу IPSec

2) Перша фаза IKE. Головною метою обміну даними, що відбувається у першій фазі IKE, є автентифікація сторін IPSec і створення захищеного каналу між сторонами, що дозволяє почати обмін IKE. У ході першої фази IKE виконуються такі дії: a) ведуться переговори щодо узгодження політики асоціацій захисту IKE між сторонами для забезпечення захисту обміну IKE. Асоціація захисту IKE отримує узгоджені параметри IKE і є двосторонньою; b) виконується автентифікований обмін за протоколом Діффі-Хеллмана, у результаті якого вибирається спільний секретний ключ для використання в алгоритмах шифрування IPSec; c) виконується автентифікація і забезпечується захист сторін IPSec; d) встановлюється захищений тунель для ведення переговорів щодо параметрів другої іншої фази IKE. Для першої фази IKE допустимі два режими:

Основний режим першої фази IKE (у цьому режимі виконуються три двосторонні обміни між ініціатором і респондентами): у ході першого обміну алгоритми, використовувані

для захисту зв'язку IKE, узгоджуються до тих пір, поки не буде досягнута відповідність для всіх асоціацій захисту IKE сторін; у процесі іншого обміну виконується алгоритм Діффі-Хеллмана, для узгодження спільного секретного матеріалу, на основі якого створюються спільні секретні ключі; у ході третього обміну виконується автентифікація сторони партнера. Ідентифікаційним значенням у даному випадку виступає IP-адреси сторони IPSec у шифрованому вигляді. Основним результатом цього режиму є узгодження параметрів асоціацій захисту IKE між сторонами з метою створення захищеного каналу для подальших обмінів IKE. SA IKE визначає параметри обміну IKE: використовуваний метод автентифікації, алгоритми шифрування і гешування, використовувана група Діффі-Хеллмана, максимальний час існування SA IKE і спільно використовувані секретні значення ключів для алгоритмів шифрування. SA IKE у пристроях кожною із сторін є двосторонніми.

Енергійний режим першої фази IKE (у цьому режимі менше і число обмінів, і число пакетів, що пересилаються при цьому, внаслідок чого потрібно менше часу для установки сеансу IPSec: у ході першого обміну майже все необхідне включається в пропоновані значення для SA IKE, відкритий ключ Діффі-Хеллмана, оказію, що підписується другою стороною, і пакет ідентифікації, який можна використовувати для того, щоб автентифікувати другу сторону за допомогою третьої сторони; одержувач відправляє назад все, що потрібно, аби завершити обмін. Ініціаторові залишається лише підтвердити обмін. Недоліком використання енергійного режиму є те, що дві сторони обмінюються інформацією до того, як створений захищений канал. Таким чином, можна підключитися до лінії і з'ясувати, хто формує нову асоціацію захисту. З іншого боку, обмін відбувається швидше, ніж в основному режимі.

3) Друга фаза IKE. Завданням другої фази IKE є узгодження параметрів SA IPSec з метою створення тунеля IPSec. У цій фазі виконуються такі дії: ведуться переговори щодо параметрів SA IPSec, що захищаються існуючою SA IKE; встановлюються SA IPSec; періодично поновлюються переговори про SA IPSec, щоб гарантувати захист; у необов'язковому порядку може виконуватися додатковий обмін Діффі-Хеллмана. Друга фаза IKE виконується лише у швидкому режимі, після того, як у результаті першої фази IKE створюється захищений тунель. Потім ведуться переговори про узгоджену політику IPSec, витягується загальний секретний матеріал для роботи з алгоритмами захисту IPSec і створюються SA IPSec. У швидкому режимі виконується обмін оказіями, які забезпечують захист від відтворення повідомлень. Оказії використовуються для того, щоб гарантувати створення нових секретних ключів і не допустити проведення атак відтворення, у результаті яких противник міг би створити «фальшиві» SA.

Швидкий режим використовується також для того, щоб домовитися про нові SA IPSec, коли виявляється перевищена межа часу існування старої SA IPSec. Базовий варіант швидкого режиму використовується для того, щоб відновити секретний матеріал, призначений для створення загального секретного ключа на основі значень, отриманих при

обміні Діффі-Хеллмана в ході першої фази. У IPSec є опція PFS (Perfect Forward Secrecy – досконала пряма секретність), що посилює захист ключів. Якщо політикою IPSec наказане використання опції PFS, то для кожного обміну у швидкому режимі потрібний новий обмін Діффі-Хеллмана, що забезпечує нові дані для ключів, внаслідок чого дані для ключів володітимуть більшою ентропією («нерегулярністю») і тому більшою стійкістю відносно криптоаналітичних атак.

Кожен обмін Діффі-Хеллмана вимагає великого числа піднесень до ступеня, що збільшує завантаження процесора і знижує загальну продуктивність системи. SA, що узгоджують у швидкому режимі, ідентифікуються IP-адресами 1KE-сторін.

У ході другої фази в рамках протоколу IKE ведуться переговори щодо перетворення IPSec (алгоритми захисту IPSec). IPSec складається з двох головних протоколів захисту і цілої низки протоколів підтримки. Перетворення IPSec і пов'язані з ними алгоритми шифрування: протокол AH (Authentication Header – заголовок автентифікації); протокол ESP; DES; 3DES та ін. При перетворенні IPSec використовується також два стандартні алгоритми гешування, що забезпечують автентифікацію даних – це MD5 та SHA-1. У рамках протоколу IKE симетричні ключі створюються за допомогою алгоритму Діффі-Хеллмана, який використовує DES, 3DES, MD5 і SHA. Він дозволяє двом сторонам узгоджувати спільний секретний ключ, не маючи досить надійного каналу зв'язку.

Спільні секретні ключі потрібні для алгоритмів DES і HMAC. Алгоритм Діффі-Хеллмана використовується в рамках IKE для створення сеансових ключів. У продуктах Cisco підтримуються 768- і 1024-бітові групи Діффі-Хеллмана.

Кожній SA IPSec привласнюється індекс SPI (Security Parameter Index – індекс параметрів захисту) – число, використовуване для ідентифікації SA IPSec. SA IPSec визначає використовуване перетворення IPSec (ESP і AH і відповідні алгоритми шифрування і гешування), межу часу існування SA IPSec у секундах або кілобайтах, вказує необхідність вживання опції PFS, IP-адреси сторін, спільні, також загальні значення секретних ключів для алгоритмів шифрування і інші параметри. Всі SA IPSec є однобічними. Один цикл узгодження SA IPSec завершується створенням двох SA – однієї вхідної і однієї вихідної.

Протоколи AH і ESP IPSec можуть діяти або в тунельному, або в транспортному режимах. Тунельний режим використовується для зв'язку між шлюзами IPSec, і, в цьому випадку, засобам IPSec доводиться створювати абсолютно новий заголовок IPSec. Транспортний режим зазвичай застосовується між клієнтом і сервером VPN, і при цьому використовується існуючий заголовок IP.

4) Передача даних. Після завершення другої фази IKE і створення асоціацій захисту IPSec у швидкому режимі, починається обмін інформацією через тунель IPSec. Пакети шифруються (зашифровуються / розшифровуються) за допомогою алгоритмів шифрування і ключів, вказаних асоціацією захисту IPSec. SA IPSec задає також межу часу свого існування в кілобайтах передаваних даних або в секундах. SA має спеціальний лічильник, значення

якого зменшується на одиницю за кожну секунду або після передачі кожного кілобайта даних.

5) Завершення роботи тунелю IPSec. SA IPSec завершують свою роботу або внаслідок їх видалення, або тому, що виявляється перевищена межа часу їх існування. Коли SA завершують роботу, відповідні ключі теж стають недійсними. Якщо для потоку даних потрібні нові SA IPSec, у рамках протоколу IKE знову виконується обмін другої фази, а якщо необхідно, то і першої. У результаті успішного їх завершення створюються нові SA ключі. Нові SA можуть створюватися і до завершення часу існування попередніх, аби потік даних міг рухатися безперервно.

Недоліком цієї технології є той факт, що з усіх властивостей віртуальної мережі технологія IPSec реалізує тільки захищеність та ізольованість адресного простору, а пропускну здатність та інші параметри QoS вона не підтримує. Крім того, серйозним мінусом протоколу IPSec є і його орієнтованість виключно на IP-протокол.

Застосування тунелів для VPN. Протоколи захищеного каналу, як правило, використовують у своїй роботі механізм *тунелювання* (рис. 9). За допомогою цієї методики пакети даних транслюються через загальнодоступну мережу як за звичайним двохточковим з'єднанням. Між кожною парою «відправник – одержувач даних» встановлюється своєрідний тунель – безпечне логічне з'єднання, що дозволяє інкапсулювати дані одного протоколу в пакети іншого.

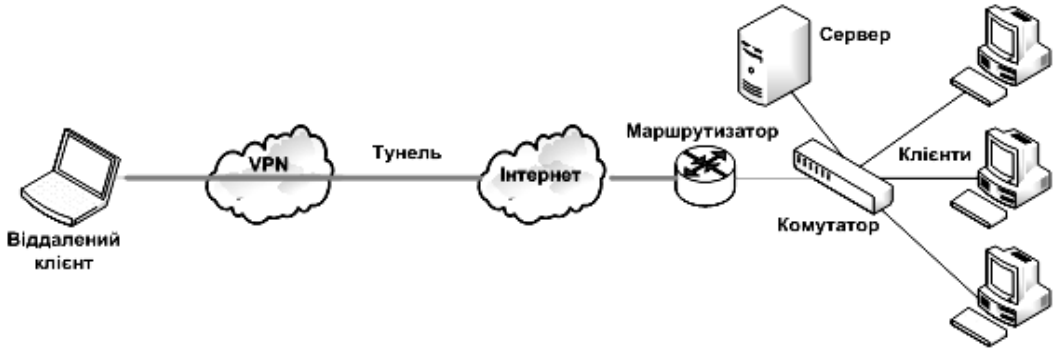

Рис. 9. VPN-тунель через мережу Інтернет

Технологія тунелювання дозволяє зашифрувати вихідний пакет повністю, разом із заголовком, а не тільки його поле даних. Такий зашифрований пакет поміщається в інший пакет з відкритим заголовком. Цей заголовок використовують для транспортування даних на ділянці загальної мережі.

У граничній точці захищеного каналу витягується зашифрований заголовок, який буде використовуватися для подальшої передачі пакета. Як правило, тунель створюється тільки на ділянці мережі загального користування, де існує загроза порушення конфіденційності і цілісності даних. Крім захисту переданої інформації, механізм тунелювання використовують для забезпечення цілісності та автентичності (при цьому захист потоку реалізується більш повно). Тунелювання застосовується також і для узгодження різних транспортних

технологій, якщо дані одного протоколу транспортного рівня необхідно передати через транзитну мережу з іншим транспортним протоколом.

Слід зазначити, що процес тунелювання не залежить від того, з якою метою він застосовується. Сам по собі механізм тунелювання не захищає дані від НСД або від спотворень, він лише створює передумови для захисту всіх полів вихідного пакету. Для забезпечення секретності переданих даних, пакети на транспортному рівні шифруються і передаються транзитною мережею.

Найчастіше для створення VPN використовується інкапсуляція протоколу PPP у який-небудь інший протокол – *IP (вже згаданий PPTP)* або *Ethernet (PPPoE)*. Останнім часом VPN використовується не тільки для створення власне приватних мереж, але й деякими провайдерами (зокрема на пострадянському просторі) для надання доступу до Інтернет.

Протокол з'єднання типу «точка-точка» (PPP). Зазвичай протокол PPP використовується для встановлення прямого зв'язку між двома вузлами мережі, причому він може забезпечити автентифікацію з'єднання, шифрування й стиснення даних. Використовується на багатьох типах фізичних мереж: нуль-модемний кабель, телефонна лінія, стільниковий зв'язок тощо. Протокол PPP розроблений для простих ліній зв'язку, які транспортують пакети між двома рівноправними вузлами – ці з'єднання надають повнодуплексне двонаправлене функціонування й беруть на себе послідовну доставку пакетів. Передбачається, що PPP надає загальне рішення для простого з'єднання територіально рознесених хостів, мостів і маршрутизаторів. До складу PPP входить ціле сімейство протоколів: керування лінією зв'язку (LCP), керування мережею (NCP), автентифікації (PAP та CHAP), багатоканальний протокол PPP (MLPPP). Сам протокол PPP був розроблений на основі HDLC і доповнений деякими можливостями. Протокол PPP також містить у собі механізми для виконання таких дій: мультиплексування мережних протоколів; конфігурування каналу; перевірки якості каналу; автентифікації; стиснення заголовків; виявлення помилок; узгодження параметрів каналу. Крім того, PPP має три головних функціональних компоненти:

1) метод інкапсуляції датаграм для послідовних каналів, основаних на протоколі HDLC;

2) протокол керування LCP, що встановлює, конфігурує й перевіряє з'єднання канального рівня, а також виконує автентифікацію;

3) протокол керування мережею NCP, що установлює й конфігурує різні протоколи мережного рівня (IP, IPX та AppleTalk).

Протокол LCP забезпечує автоматичне налаштування інтерфейсів на кожному кінці (наприклад, установка розміру пакетів, опцій формату інкапсуляції тощо) і опціонально виконує автентифікацію. Також варто зазначити, що протокол LCP працює поверх PPP, тобто початковий PPP зв'язок повинен бути до роботи LCP. З огляду на те, що в PPP входить LCP протокол, з'являється можливість управління такими LCP параметрами:

– *Автентифікація.* Документ RFC 1994 описує протокол CHAP, який є кращим для проведення автентифікації у PPP, хоча протокол PAP іноді ще використовується. Проте у налаштуваннях можна й відмовитись від будь-якої подібної перевірки. При використанні будь-якого з протоколів (PAP або CHAP) має місце двосторонній процес, у якому пара ідентифікатор / пароль постійно посилається пристрою автентифікації доти, поки не будуть визнані права на доступ викликаючої сторони або з'єднання не буде припинено. Варто зауважити, що при використанні протоколу PAP, такий процес не забезпечує повної надійності. Якщо до каналу підключити аналізатор протоколу, то пароль буде видно у вигляді відкритого тексту. При використанні протоколу PAP немає захисту від багаторазового зчитування запитів (якщо є програмний або апаратний перехоплювач трафіку, фізично підключений до каналу, і пакет перехоплюється, то його можна потім використовувати для підтвердження своєї автентифікації, шляхом направлення його безпосередньо до мережі й відтворення перехоплених пакетів).

Якщо потрібно більш надійний метод контролю доступу, то як метод автентифікації варто використовувати не протокол PAP, а саме CHAP: Протокол PAP варто використовувати тільки в тому випадку, якщо це єдиний метод автентифікації, що підтримує станція. Протокол PAP є односторонньою перевіркою в тому випадку, коли вона здійснюється між вузлом і сервером доступу, а якщо така перевірка відбувається між маршрутизаторами, то це двосторонній процес. При використанні ж перевірки за протоколом CHAP сервер доступу після встановлення каналу PPP посилає повідомлення-запит на вилучений вузол. Вилучений вузол відповідає значенням, обчисленим з використанням односторонньої геш-функції (зазвичай за допомогою алгоритму MD5). Сервер доступу перевіряє отриману відповідь і порівнює її зі своїм заздалегідь обчисленим значенням цієї ж величини. Якщо величини збігаються, то автентифікація вважається підтвердженою. У противному випадку з'єднання негайно переривається. Іншим варіантом для організації автентифікації є використання протоколу EAP.

– *Стиснення.* За рахунок стиснення даних у кадрі значно збільшується пропускна здатність PPP-з'єднання. Найбільш відомими алгоритмами стиснення PPP кадрів є Stacker та Predictor. Перший алгоритм, що заснований на алгоритмі Lempel-Ziv (LZ), аналізує дані і замість відправлення вихідного потоку відразу відправляє блоки даних з інформацією про те, де певна послідовність біт зустрічається у потоці даних, а потім передає відповідні послідовності. Приймаюча сторона використовує одержувану в такий спосіб інформацію для повторного складання даних. Алгоритм Predictor перевіряє чи не були дані вже стиснуті: якщо були, то дані просто пересилаються і час на перевірку можливості стиснення уже стиснених даних не затрачається. У маршрутизаторах Cisco зазвичай застосовується алгоритм MPPCP, який теж базується на LZ.

– *Виявлення помилок.* Включає Quality-Protocol і допомагає виявити петлі зворотного зв'язку за допомогою Magic Numbers (RFC 1661).

– *Багатоканальність.* Multilink PPP (MLPPP, MPPP, MLP) надає методи для поширення трафіку через кілька фізичних каналів, маючи одне логічне з'єднання. Цей варіант дозволяє розширити пропускну здатність і забезпечує балансування навантаження.

PPTP. PPTP – це протокол тунелювання «точка-точка», розроблений фірмою Microsoft. Фактично, цей протокол є розширенням протоколу PPP, який використовується в технологіях глобальних мереж та під час утворення з'єднання через комутоване середовище (рис. 10).

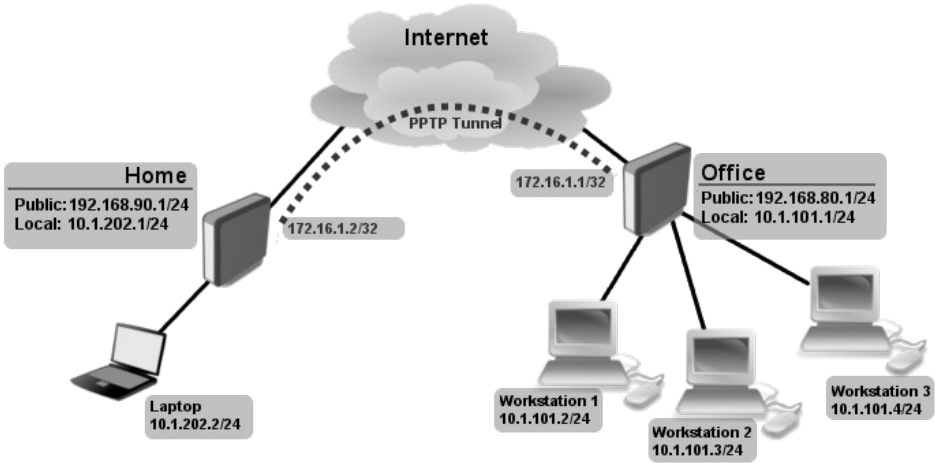

Рис. 10. Варіант побудови тунелю за протоколом PPTP

PPTP поміщає (інкапсулює) кадри PPP в IP-пакети для передачі глобальною IP-мережею, наприклад Інтернет. PPTP може також використовуватися для організації тунелю між двома локальними мережами. PPTP використовує додаткове TCP-з'єднання для обслуговування тунелю. Протокол вважається менш безпечним, ніж IPSec. PPTP працює, установлюючи звичайну PPP сесію із протилежною стороною за допомогою протоколу GRE. Друге з'єднання на TCP- порту 1723 використовується для ініціації й керування GRE-з'єднанням. PPTP складно перенаправляти за мережний екран, тому що він вимагає одночасного встановлення двох мережних сесій. PPTP-трафік може бути зашифрований за допомогою MPPE. Для автентифікації клієнтів можуть використовуватися різні механізми, найбільш безпечними з них є MS-CHAPv2 і EAP-TLS. Першою PPTP реалізувала компанія Cisco, а пізніше ліцензувала за цією технологію корпорацію Microsoft. Проте PPTP вдалося домогтися популярності у більшій мірі завдяки тому, що це перший протокол тунелювання, який був підтриманий саме корпорацією Microsoft.

Усі версії Microsoft Windows, починаючи з Windows 95 OSR2, включають у свій склад PPTP-клієнт, однак існує обмеження на два одночасно вихідних з'єднання. А сервіс вилученого доступу для Microsoft Windows містить у собі PPTP сервер. Донедавна в дистрибутивах Linux була відсутня повна підтримка PPTP через побоювання патентних претензій з приводу протоколу MPPE. Уперше повна підтримка MPPE з'явилася в Linux 2.6.13. Офіційно підтримка PPTP була почата з версії ядра Linux 2.6.14. Проте, сам факт застосування MPPE в PPTP фактично не забезпечує безпеку протоколу PPTP. Операційна

система FreeBSD підтримує PPTP протокол, використовуючи як сервер PPTP порт mpd (/usr/ports/net/mpd), використовуючи підсистему netgraph.

У ролі клієнта PPTP у системі FreeBSD може виступати або порт pptpclient (/usr/ports/net/pptpclient), або порт mpd, що працює в режимі клієнта. MicrosoftWindowsMobile 2003 і більш нові версії цієї ОС також підтримують PPTP. Протокол PPTP не можна вважати прийнятним, з погляду інформаційної безпеки, як мінімум, без вживання додаткових заходів щодо забезпечення інформаційної безпеки каналів зв'язку, або без застосування додаткових засобів захисту інформації (наприклад додаткового шифрування даних). Таким чином, PPTP не слід застосовувати у загальнодоступних мережах для забезпечення конфіденційності та/або збереження важливої (критичної) інформації.

PPPoE. Технологія використання стеку PPP у мережі Ethernet, яка на цей момент визначається документом RFC 2516 (розробниками є компанії RedBack Networks, RouterWare, UUNET та ін.). Використання цього протоколу надає провайдерам послуг Інтернет нові можливості щодо організації і обліку доступу користувачів до мережі. Це особливо актуально для тих провайдерів, які планують або вже пропонують своїм користувачам доступ до Інтернет за допомогою мережі Ethernet, наприклад, в сучасних житлових комплексах. Технологія PPPoE на сьогодні є однією з найдешевших при наданні користувачам доступу до послуг Інтернет у житлових комплексах на базі Ethernet і при використанні технології DSL. Оскільки принципом роботи PPPoE є встановлення з'єднання «точка-точка» поверх загального середовища Ethernet, то процес функціонування PPPoE має бути розділений на дві стадії. У першій стадії два пристрої повинні повідомити один одному свої адреси і встановити початкове з'єднання, а в другій – запустити сесію PPP.

1) Стадія встановлення з'єднання. Спочатку клієнт посилає широкомовний запит (адреси призначення – Broadcast Address) (PADI, PPPoE Active Discovery Initiation) на пошук сервера із службою PPPoE. Цей запит отримують всі абоненти мережі, але відповість на нього лише той, у кого є підтримка служби PPPoE. У відповідь пакет від BRAS (PADO, PPPoE Active Discovery Offer) посилається у клієнту, але якщо у мережі є багато пристроїв зі службою PPPoE, то клієнт отримає багато пакетів PADO. У цьому випадку, ПЗ клієнта вибирає необхідний йому концентратор доступу і посилає йому пакет (PADR, PPPoE Active Discovery Request) з інформацією про необхідну службу (необхідний клас обслуговування залежить від послуг провайдера) ім'я провайдера і т.д. Після отримання запиту, BRAS готується до PPP сесії і посилає клієнтові пакет PADS (PPPoE, Active Discovery Session-confirmation). Якщо усі запрошувані клієнтом служби доступні (до складу цього пакету входить унікальний номер сесії, привласнений BRAS), то починається другий етап – стадія встановлення сесії. Якщо потрібні клієнту послуги не можуть бути надані, клієнт отримує пакет PADS з вказівкою помилки у запиті послуги.

2) Стадія встановлення сесії. Сесія починається з використання пакетів PPP. При встановленні PPP-сесії абонент може бути автентифікований за допомогою протоколу

CHAP. Після цього BRAS обмінюється інформацією, отриманою від абонента, з RADIUS сервером і абонентові можна призначити динамічну адресу IP з пулу адреса BRAS, встановити налаштування шлюзу і DNS-сервера. При цьому, на BRAS клієнту відповідно ставиться віртуальний інтерфейс. Завершення з'єднання PPPoE відбувається за ініціативою клієнта або BRAS за допомогою посилання пакету PADT (PPPoE, Active Discovery Terminate).

У протоколі PPPoE передбачені деякі додаткові функції, наприклад, захист від DoS-атак. Такий захист реалізований шляхом додавання в пакети PADI спеціального поля AC-Cookie, яке дозволяє BRAS обмежувати кількість одночасних сесій PPPoE на одного клієнта. Важливо також відзначити, що протокол PPPoE не залежить від типу технології доступу (xDSL, кабельні модеми, системи бездротового доступу, комбіновані мідно-оптичні системи типу FTTC тощо). Крім того, в PPPoE є ще одна корисна властивість, яка надає кінцевим користувачам право вибору типу мережевої послуги. Цю функцію часто називають функцією додаткового вибору послуги. Вона дозволяє кінцевим користувачам змінювати адресат мережі на вимогу й навіть мати безліч сеансів зв'язку з різними мережами зв'язку одночасно з одного приміщення користувача через єдину лінію доступу.

Протокол L2TP. PPTP є технологією компанії Microsoft для створення віртуальних каналів зв'язку усередині колективної мережі. PPTP разом з системами шифрування і автентифікації створює приватну безпечну мережу. Cisco Systems розробила протокол, аналогічний PPTP, під назвою *Layer Two Forwarding (L2F),* але для його підтримки потрібне обладнання Cisco на обох кінцях з'єднання. Згодом компанії Microsoft і Cisco об'єднали кращі якості протоколів PPTP і L2F і розробили протокол *L2TP.* Як і PPTP, L2TP дозволяє користувачам створити в Інтернет PPP-лінію зв'язку, що поєднує ISP (Internet Service Provider) і корпоративний сайт.

Протокол L2TP є тунельним протоколом другого рівня, підтримка якого вперше була реалізована у клієнтській і серверній ОС Windows 2000. На відміну від PPTP, L2TP на серверах під керуванням Windows Server 2003 (та більш нових версіях) не використовує MPPE для шифрування датаграм PPP. L2TP використовує засоби шифрування, які надаються IPSec. Комбінацію L2TP і IPSec називають L2TP / IPSec. Така комбінація забезпечує роботу служб VPN, що виконують інкапсуляцію й шифрування частин даних. L2TP та IPSec повинні підтримуватися як на VPN-Клієнті, так і на VPN-Сервері. Клієнтська підтримка L2TP вбудована у клієнт вилученого доступу Windows XP, а підтримка L2TP VPN-Серверами – в ОС Windows Server.

Протокол L2TP установлюється разом із протоколом TCP/IP. Залежно від параметрів, обраних у майстрі налаштування сервера маршрутизації й вилученого доступу, протокол L2TP настроюється для 5 або 128 портів. Повідомлення L2TP шифрується з використанням алгоритму DES або 3DES за допомогою ключів шифрування, створених у процесі узгодження IKE. Можна також використовувати нешифроване L2TP-Підключення, при

якому кадри PPP пересилаються у відкритому вигляді. Однак, для віртуальних приватних підключень в Інтернет застосовувати нешифровані підключення не рекомендується, тому що вони не забезпечують необхідного рівня конфіденційності даних.

Протокол GRE (Generic Routing Encapsulation – загальна інкапсуляція маршрутів). Розроблений Cisco тунельний протокол, що забезпечує інкапсуляцію багатьох типів протокольних пакетів у тунелі IP, створює віртуальний двоточковий зв'язок з маршрутизаторами Cisco у вилучених точках IP-мережі. На рис. 1.5.5 зображено пряме з'єднання сегментів мережі 192.168.1.0/24 та 192.168.3.0/24 за протоколом GRE (ніби вони з'єднані прямим лінком).

Протокол MPPE (Microsoft Point-to-Point Encryption – протокол шифрування двоточкового з'єднання). Цей протокол є засобом перекладу пакетів PPP (застосовується поверх протоколу PPP) у шифровану форму. Дозволяє створити захищений VPN-зв'язок або вилучену мережу. Для забезпечення конфіденційності даних у MPPE використовується потоковий шифр RC4. Проте, MPPE підтримується далеко не всіма побутовими маршрутизаторами і, на сьогодні, є частим джерелом несумісності обладнання при роботі у локальних будинкових мережах.

Наприклад, деякі з Інтернет-шлюзів D-Link підтримують автентифікацію тільки PAP і CHAP і не підтримують шифрування MPPE.

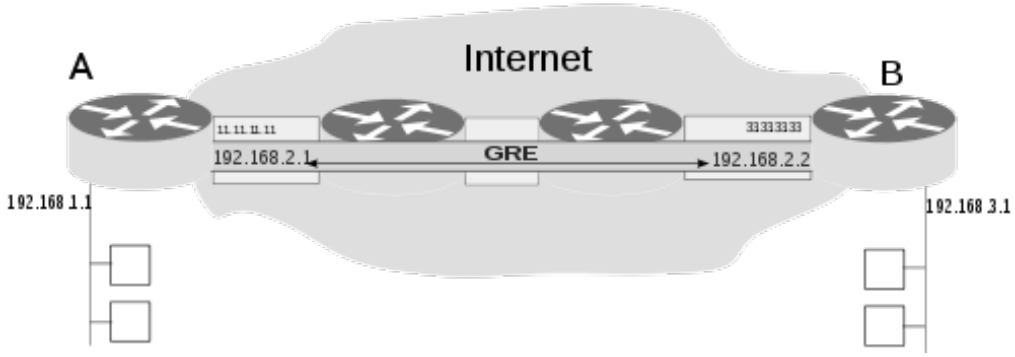

Рис. 11. Приклад роботи тунелю за протоколом GRE

До основних переваг технології VPN варто віднести: високі швидкості підключення; надійність системи віртуальних каналів зв'язку; гарантія безпеки передачі даних; відсутність дистанційних обмежень; оперативність і простота підключення нових користувачів і мереж; гнучке налаштування конфігурації мережі; відсутність необхідності витрат на закупівлю, монтаж і конфігурацію серверів віддаленого доступу і модемів; низька вартість орендованих каналів і комунікаційного устаткування.

Контрольні запитання

1) Що таке VPN? У чому їх основні переваги над звичайним приватними мережами?

2) Які існують види VPN мереж за різними базовими ознаками?

3) У чому особливість технології IPSec? Фази роботи IPSec та її основні компоненти.

4) У чому полягає технологія тунелювання? Яким чином вона реалізовується?

5) Які сучасні протоколи шифрування застосовуються у VPN мережах?

6) У чому полягають особливості та функціональне призначення протоколів PPTP, PPPoE, GRE, MPPE, L2TP?

7) Які є фази протоколу IKE? У чому їх суть?

8) Особливості побудови VPN мереж на базі MPLS.

9) Автентифікація на базі протоколів PAP та CHAP.

10) Які основні задачі розв’язує технологія IPSec при побудові VPN мереж?

Тема 6. Симетричні та асиметричні системи шифрування електронних інформаційних ресурсів

Основні аспекти криптографічного захисту інформації. Серед усього спектру методів захисту інформації в ІКС особливе місце займають криптографічні методи, які, на відміну від інших, спираються лише на властивості самої інформації і не використовують властивості її матеріальних носіїв, особливості вузлів її оброблення, передачі та зберігання. Широке використання і постійне збільшення об'єму інформаційних потоків викликає постійне зростання інтересу до криптографії. Останнім часом збільшується роль саме програмних криптографічних засобів, які не потребують великих фінансових витрат порівняно з апаратними криптосистемами.

Взагалі *«криптографія»* – це грецьке слово, що походить від слів kryptos (таємний, схований) та graphy (запис). *Криптографією* називається наука, що включає методи та засоби перетворення даних з метою приховування (маскування) змісту інформації для гарантування її конфіденційності та цілісності (відповідно, криптоаналіз орієнтований на зламування шифротекстів).

Крім забезпечення конфіденційності інформації, сьогодні криптографія застосовується для розв'язання таких задач:

– *перевірка справжності відправника – автентифікація* (одержувач може встановити відправника, а зловмисник не може під нього маскуватися);

– *забезпечення цілісності* (отримувач може перевірити несанкціоновану модифікацію у тексті, а зловмисник не може видати підроблений текст за справжній);

– *не заперечення авторства* (відправник не може у подальшому заперечувати відсилку даних).

У сучасні криптографії можна виділити такі базові розділи:

1) Симетрична криптографія (криптографія із секретним ключем) – наука, що вивчає криптографічні методи, у яких використовується один секретний ключ для зашифрування і розшифрування.

2) Асиметрична криптографія (криптографія з відкритим ключем) – наука, що вивчає криптографічні методи, у яких використовуються роздільні ключі для реалізації процесу зашифрування і розшифрування (відкритий і секретний). У таких методах секретність повідомлень ґрунтується на складності обчислення ключа за деякою функціонально залежною від нього інформацією, що передається різними каналами зв'язку.

3) Квантова криптографія – наука, що вивчає методи захисту систем зв'язку і базується на постулатах квантової механіки, об'єкти якої (здебільшого це фотони) забезпечують процеси безпечної передачі інформації (див. тема 2.4).

Вимоги до сучасних криптосистем:

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

– 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 чітку нижню оцінку і виходити за межі можливостей сучасних та перспективних комп'ютерних систем та мереж;

– 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 у процесі шифрування;

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

Принципи криптографії

1) Принцип рівної міцності захисту. На шляху від одного легітимного користувача до іншого інформація може захищатись різними способами у залежності від загроз, що виникають. Так утворюється ланцюг захисту інформації з ланками різного типу. Зловмисник прагне знайти найслабкішу ланку, щоб з найменшими витратами отримати бажану інформації. Таким чином, безглуздо робити якусь ланку дуже міцною, якщо є слабкі ланки.

2) Принцип доцільності захисту. На сучасному рівні технічного розвитку засоби зв'язку, засоби перехоплення повідомлень, а також засоби захисту інформації вимагають занадто великих витрат. Тому, існує проблема співвідношення вартості інформації, витрат на її захист та витрат на її здобування.

Перш ніж захищати інформацію криптографічними методами, треба відповісти на два таких питання:

a) чи отримає порушник внаслідок атаки інформацію, що буде більш цінною, ніж вартість самої атаки?

b) чи є інформація, яку захищає її власник (легітимний користувач), більш цінною, ніж вартість захисту?

Відповідь на ці два питання визначає доцільність захисту й вибір необхідних 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

порушник уже зламав шифр і вільно читає шифровані повідомлення. Саме тому, в сучасних шифрах використовують ключі. При цьому вважають, що сам шифр (за виключенням ключа шифрування) є відомим зловмиснику і доступним для вивчення. Оригінальність подання повідомлення забезпечується тільки періодично змінюваним ключем. Знання ключа дозволяє швидко та просто відновити початковий текст, а без знання ключа розшифрування 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.

5) Принцип Керкхоффса. Стійкість сучасного шифру має визначатись, у 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 легше перешкоджати зловмиснику, змінюючи їх досить часто.

6) Принцип використання різноманітних шифрів. Не існує єдиного шифру, що підходить до всіх випадків. Вибір конкретного шифру залежить від низки чинників – від особливостей інформації, її цінності та обсягів, а також від потрібної швидкості її передачі, тривалості захисту, можливостей зловмисників і власників щодо захисту своєї інформації тощо.

Не зважаючи на великий спектр криптографічних методів і засобів сьогодення, криптографія має низку проблем, вирішення яких є важливим для забезпечення безпеки інформації в ІКС. Серед **проблем криптографії** варто відзначити такі**:**

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

2) Гіпотетична стійкість криптосистем з відкритим ключем. Використання асиметричної криптографії базується на гіпотетичній неможливості розв'язання певного класу математичних задач, які, з огляду на розвиток сучасних обчислю-вальних потужностей (п. 1), можуть бути розв'язаними у недалекому майбутньому.

3) Проблема розподілу ключів шифрування – ключі мають бути доставленими до легітимних користувачів вчасно і за умов суворої секретності – це зробити досить складно і здебільшого (принаймні у нашій державі) для вирішення цієї проблеми використовують не цілком надійні методи «довірених кур'єрів» (висока вартість та залежність від людського чинника) та методи асиметричної криптографії (див. п. 2).

4) Складність оцінки ефективності сучасних криптографічних засобів. Існуючі криптографічні засоби захисту інформації мають закриту інфраструктуру, що ускладнює їх аналіз, та знижує об'єктивність оцінки їх ефективності.

Блокові шифри

Переважна більшість сучасних алгоритмів шифрування працюють вельми схожим чином: над шифрованим текстом виконується якесь перетворення за участю ключа шифрування, яке повторюється певну кількість разів (раундів). При цьому, *за виглядом перетворення (за структурою), що повторюється,* алгоритми шифрування прийнято ділити на чотири категорії:

1) Алгоритми на основі мережі Фейстеля

Мережа Фейстеля (Feistel Network) передбачає розбиття оброблюваного блоку даних на декілька субблоків (частіше всього – на два), один з яких обробляється певною функцією *f* і накладається на один або декілька останніх субблоків. На рис. 12 приведена типова структура алгоритмів на основі мережі Фейстеля:

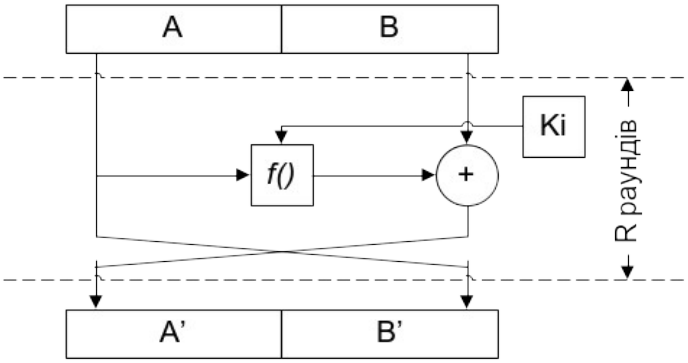

Рис. 12. Мережа Фейстеля

Додатковий аргумент функції *f*, позначений на рис. 12 як K_i, називається ключем раунду. Ключ раунду є результатом оброблення ключа шифрування процедурою розширення ключа, завдання якої – здобуття необхідної кількості ключів K_i з вихідного ключа шифрування відносно невеликого розміру (сьогодні достатнім для ключа симетричного шифрування у типових криптосистемах вважається розмір 128 бітів). У простих випадках процедура розширення ключа просто розбиває ключ на декілька фрагментів, які по черзі використовуються у раундах шифрування; істотно частіше процедура розширення ключа є досить складною, а ключі K_i залежать від значень більшості бітів вихідного ключа шифрування.

Накладення обробленого субблоку на необроблений найчастіше виконується за допомогою логічної операції XOR (див. рис. 12). Досить часто замість XOR використовується складання за модулем $2n$, де n – розмір субблоку в бітах. Після накладення, субблоки міняються місцями, тобто в наступному раунді алгоритму обробляється вже інший субблок даних. Така структура алгоритмів шифрування отримала свою назву за іменем Хорста Фейстеля (H. Feistel) – одного з розробників алгоритму шифрування Lucifer і розробленого на його основі алгоритму DES – колишнього стандарту шифрування США. Обидва зазначені алгоритми мають структуру, аналогічну показаній на рисунку. Серед інших алгоритмів, заснованих на мережі Фейстеля, можна відзначити

вітчизняний стандарт шифрування ДСТУ ГОСТ 28147:2009, а також інші відомі алгоритми – RC5, Blowfish, TEA, CAST-128 і т.д.

На мережі Фейстеля заснована більшість сучасних алгоритмів шифрування – завдяки їх перевагам, серед яких варто відзначити такі:

1) алгоритми на основі мережі Фейстеля можуть бути сконструйовані таким чином, що для зашифрування і розшифрування може використовуватися один і той же код алгоритму – різниця між цими операціями може полягати лише в порядку використання ключів K_i; така властивість алгоритму найбільш корисна при його апаратній реалізації або на платформах з обмеженими ресурсами;

2) такі алгоритми є найбільш вивченими (дослідженими) – їм присвячена величезна кількість криптоаналітичних досліджень, що є безперечною перевагою як при розробці алгоритму, так і при його аналізі.

Існує і більш складна структура мережі Фейстеля, приклад якої наведений на рис. 13. Така структура називається *узагальненою* або *розширеною мережею Фейстеля* і використовується істотно рідше за традиційну мережу Фейстеля. Прикладом такої мережі Фейстеля може служити відомий алгоритм RC6.

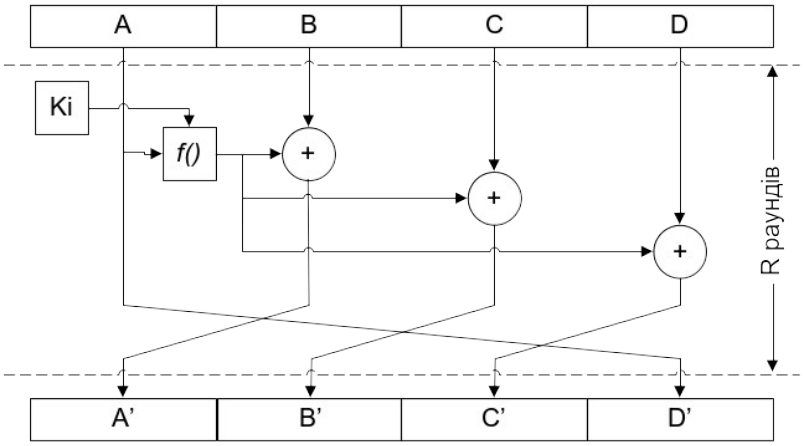

Рис. 13.Розширена мережа Фейстеля

2) Алгоритми на основі SP-мереж

На відміну від мережі Фейстеля, *SP-мережі (Substitution-Permutation Network),* тобто *мережі замін-перестановок,* обробляють за один раунд цілий шифрований блок. Оброблення даних зводиться, в основному, до замін (наприклад, коли фрагмент вхідного значення замінюється іншим фрагментом відповідно до таблиці замін, яка може залежати від значення ключа K_i) і перестановок, залежних від ключа K_i (спрощена схема показана на рис. 14). З огляду на те, що такі операції характерні й для інших типів алгоритмів шифрування, тому назва SP-мережі є достатньо умовною.

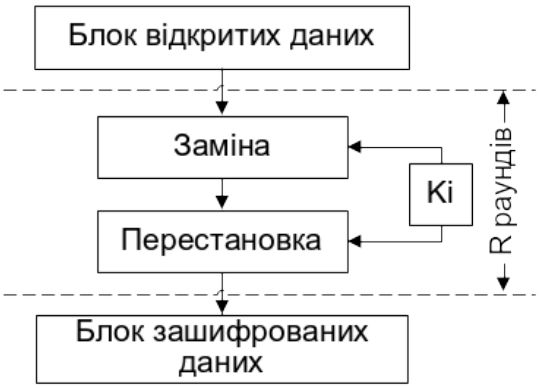

Рис. 14. Схема SP-мережі

Сьогодні SP-мережі є менш поширеними, ніж мережі Фейстеля. Яскравими представниками таких алгоритмів є Serpent та SAFER+.

3) Алгоритми із структурою «квадрат»

Для структури «квадрат» (Square) характерне представлення шифрованого блоку даних у вигляді двовимірного байтового масиву. Криптографічні перетворення можуть виконуватися над окремими байтами масиву, а також над його рядками або стовпцями. Ця структура отримала свою назву від алгоритму Square, який був розроблений у 1996 р. В. Ріджменом і Дж. Деймен – майбутніми авторами алгоритму Rijndael, що став в США новим стандартом шифрування AES після перемоги на відкритому конкурсі. Алгоритм Rijndael також має Square-подібну структуру; крім того, як приклад можна привести алгоритми SHARK (раніше розробка Ріджмена і Деймена) і Crypton. Деякі вчені не виділяють такого типу алгоритмів і відносять шифри SHARK та Rijndael до SP-мереж. Недоліком таких алгоритмів є їх недостатня вивченість, проте це не завадило алгоритму Rijndael стати новим стандартом шифрування США.

4) Алгоритми з нестандартною структурою

Винахідливість безмежна, тому класифікувати певним чином усі можливі варіанти алгоритмів шифрування є дуже складно. Існують такі алгоритми, які неможливо зарахувати ні до одного з перерахованих типів. Як приклад алгоритму з нестандартною структурою можна привести унікальний за своєю структурою алгоритм FROG, у кожному раунді якого за досить складними правилами виконується модифікація двох байтів шифрованих даних.

Чіткі границі між описаними вище структурами не визначені, тому досить часто зустрічаються алгоритми, що зараховуються різними експертами до різних типів структур. Наприклад, алгоритм CAST-256 відноситься його автором до SP-мереж, а багатьма експертами називається розширеною мережею Фейстеля. Інший приклад – алгоритм HPC, названий його автором мережею Фейстеля, але експерти відносять його до алгоритмів з нестандартною структурою.

Потокові шифри

Потоковий шифр – це симетричний шифр, які шифрує кожен символ відкритого тексту незалежно від інших символів. У основі таких шифрів є шифр XOR (рис. 15), з тією відмінністю, що гама для шифру XOR формується за певним алгоритмом, який є криптостійким ГПВП.

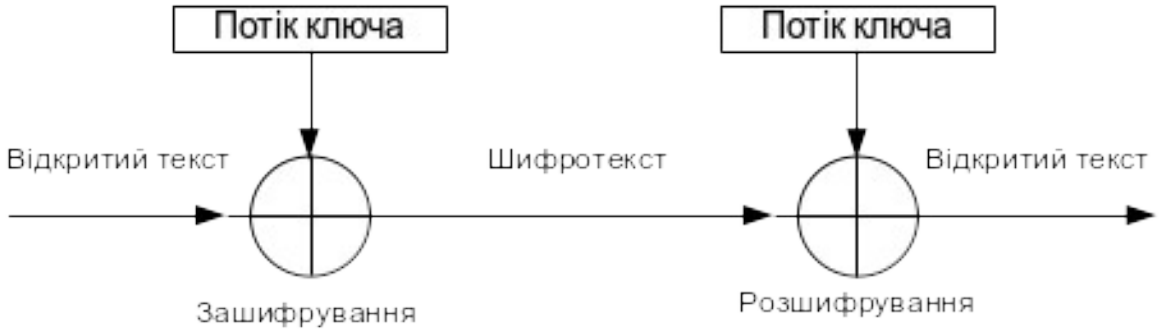

Рис. 15. Типова схема роботи потокового шифру

Історична довідка. Потокові шифри на базі зсувних регістрів активно використовувалися у роки Другої світової війни, ще задовго до появи електроніки, вони були прості у проектуванні та реалізації. 1965 р. Е. Селмер, головний криптограф норвезького уряду, розробив теорію послідовності зсувних регістрів. Пізніше С. Голомб, математик Агентства Національної Безпеки США, написав книгу під назвою «Shift Register Sequences» («Послідовності зсувних регістрів»), у якій виклав свої основні досягнення у цій галузі, а також досягнення Е. Селмера. Велику популярність потоковим шифрів принесла робота К. Шеннона, опублікована у 1949 р., у якій Шеннон довів *абсолютну стійкість шифру Вернама.* У шифрі Вернама ключ має довжину, рівну довжині самого переданого повідомлення. Якщо кожен біт ключа вибирається випадково, то розкрити шифр неможливо (тому що всі можливі відкриті тексти будуть рівноймовірнісними). Шифри, в яких довжина ключа менша від довжини тексту, згідно з Шенноном, не можуть бути «ідеально безпечними». Для таких шифрів вводять інше розуміння безпечності (практична стійкість).

Типи потокових шифрів

Потоковий шифр породжує послідовність елементів потоку ключа базуючись на внутрішньому стані. Цей стан оновлюється двома способами: якщо стан змінюється незалежно від відкритого тексту або шифротексту повідомлення, шифр позначають *синхронним (Synchronous)* потоковим шифром. Натомість, потокові шифри такі, що *самосинхронізуються (Self-synchronising)* оновлюють стан на основі попередніх цифр шифротексту.

Синхронні потокові шифри. У синхронному потоковому шифрі потік ПВП породжується незалежно від відкритого тексту та шифротексту і поєднується з відкритим текстом (для шифрування) або шифротекстом (для розшифрування). У найпоширенішій формі використовуються двійкові числа (біти) і потік ключа поєднується з відкритим

текстом за допомогою XOR. Тут вживається термін *двійковий адитивний потоковий шифр (Binary Additive Stream Cipher).*

У синхронних шифрах, відправник і отримувач повинні «йти точно в ногу» для успішного розшифрування. Якщо якесь число додане або видалене з потоку під час передачі – синхронізація втрачається. Для відновлення синхронізації з ціллю отримання правильного відкритого тексту автоматично застосовуються різні зсуви. Інший підхід полягає у використанні позначок у шифротексті з визначеною регулярністю. Однак, якщо число пошкоджене, тоді це вплине лише на одне число у відкритому тексті і помилка не поширюється на інші частини повідомлення. Ця властивість корисна у випадку високої схильності до помилок під час передачі. Однак, це робить менш імовірним виявлення помилки без додаткових механізмів. Більше того, через цю властивість, потокові шифри дуже уразливі до активних атак – якщо нападник може змінити число в шифротексті, він може змінити біт і у відкритому тексті (наприклад, зміна біту в шифротексті спричиняє зміну того самого біту у відкритому тексті).

Потокові шифри, що самосинхронізуються. Інший підхід використовує декілька з N попередніх чисел шифротексту для обчислення потоку ключа. Така схема відома як потокові шифри, що само синхронізуються (асинхронні потокові шрифти, шифротекст з автоключем). Ідею асинхронних шифрів запатентували у 1946 р. Перевага таких шифрів полягає у тому, що отримувач автоматично синхронізується з генератором потоку ключів після отриманні N чисел шифротекст – це полегшує відновлення у випадку, якщо до потоку додане чи видалене число.

Головною *перевагою асинхронних шифрів* є розмішування статистики відкритого тексту. Так як кожен знак відкритого тексту впливає на наступний шифротекст, статистичні властивості відкритого тексту поширюються на весь шифротекст. Отже, такий шифр може бути стійкішим до атак на основі надмірності відкритого тексту, ніж синхронні потокові шифри. Недоліками є:

1) поширення помилки (кожному неправильному біту шифротексту відповідають N помилок у відкритому тексті);

2) чутливі до розкриття повторною передачею тощо.

Загальна ідея потокового шифру полягає у тому, що на основі симетричного ключа виробляється ключова послідовність або *гама.* Принцип *зашифрування гамуванням* – це генерація гами шифру за допомогою датчика ПВП і накладення отриманої гами на відриті дані оберненим чином (наприклад, використовуючи додавання за модулем 2). Процес *розшифрування даних* – це повторна генерація гами шифру при відомому ключі й накладення такої гами на зашифровані дані. Таким чином, можна виділити *потокові шифри на основі ГПВП.*

Потокові шифри, зазвичай, більш продуктивні, ніж блокові й використовуються для шифрування мови, мережевого трафіку та інших даних із заздалегідь відомою довжиною.

Але потокові шифри не повною мірою підходять для програмних реалізацій, оскільки шифрують (зашифровують / розшифровують) лише по одному біту даних. Блокові ж шифри легко реалізовувати програмно, оскільки вони дозволяють уникнути значних маніпуляцій з бітами й оперують зручними для комп'ютера блоками даних. З іншого боку, потокові шифри простіші за блокові для апаратної реалізації.

Серед сучасних потокових шифрів варто відзначити такі: RC4 (використовується у HTTPS і WEP), CSS, Salsa20 (стійкий, швидкий, крім ключа використовує так званий нонс), SEAL, PANAMA, HC-256, Achterbahn-128/80 та ін.

Конкурс AES

Алгоритм шифрування DES був стандартом симетричного шифрування США з 1979 р. і до прийняття нового стандарту у вигляді алгоритму AES. Фактично перші реальні кроки щодо заміни стандарту шифрування були зроблені у 1997 р., коли NIST (National Institute of Standards and Technology) оголосив про проведення відкритого конкурсу алгоритмів шифрування, переможець якого повинен був стати новим стандартом симетричного шифрування США.

У конкурсі могли взяти участь будь-які організації або приватні особи, у тому числі й ті, що знаходяться за межами США. І дійсно, список учасників конкурсу виявився вельми різноманітним – серед авторів алгоритмів-претендентів були: всесвітньо відомі криптологи, наприклад, інтернаціональний колектив авторів алгоритму Serpent – Р. Андерсон, Елі Бі-хам та Л. Кнудсен; організації, що давно працюють у цій галузі і володіють як багатим досвідом розробки криптоалгоритмів, так і сильними фахівцями, наприклад, американська фірма Counterpane – автор алгоритму Twofish; всесвітньо відомі корпорації, що володіють великим науковим потенціалом, наприклад, німецький телекомунікаційний гігант Deutsche Telekom з алгоритмом MAGENTA; освітні установи, відомі своїми досягненнями у галузі криптографії, наприклад, Католицький Університет (м. Лювен, Бельгія) з алгоритмом Rijndael; маловідомі організації, наприклад, фірма Tecnologia Apropriada (автор алгоритму FROG) з Коста-Ріки.

NIST встановив всього *дві обов'язкові вимоги* до алгоритмів-учасників:

1) 128-бітовий розмір блоку шифрованих даних;

2) не менше трьох підтримуваних алгоритмом розмірів ключів шифрування (128, 192 і 256 бітів).

Проте, до майбутнього стандарту шифрування, було набагато більше рекомендаційних вимог. Оскільки задовольнити обов'язкові вимоги було досить просто, аналіз алгоритмів і вибір з них кращого проводився саме за його відповідності «необов'язковим» характеристикам. *Побажання NIST* були, зокрема, такими:

– алгоритм має бути стійким проти криптоаналітичних атак, відомих на момент проведення конкурсу;

– структура алгоритму має бути зрозумілою, простою і обґрунтованою, що, по-перше, полегшувало б вивчення алгоритму фахівцями, а, по-друге, гарантувало б відсутність упроваджених авторами алгоритму «закладок»;

– мають бути відсутніми слабкі і еквівалентні ключі;

– швидкість шифрування даних має бути високою на усіх потенційних апаратних платформах – від 8-бітових до 64-бітових;

– структура алгоритму повинна дозволяти розпаралелювання операцій у багатопроцесорних системах і апаратних реалізаціях;

– алгоритм повинен пред'являти мінімальні вимоги до оперативної і енергонезалежної пам'яті;

– не повинно бути обмежень на використання алгоритму, зокрема, у різних стандартних режимах роботи, як основа для побудови геш-функцій, ГПВП і так далі.

Ці вимоги виявилися досить жорсткими і такими, що частково заперечують одна одну. Кожен конкретний алгоритм, з тих, що брали участь в конкурсі, був певним компромісом з боку авторів (між пред'явленими вимогами). Заявки від учасників конкурсу приймалися протягом 18 місяців, після чого всі прислані на конкурс алгоритми вивчалися і обговорювалися як у самому інституті NIST, так і всіма, хто бажав. Варто сказати, що до NIST прийшли немало відгуків, усі вони знаходяться у відкритому доступі і їх можна поглянути на web-сайті інституту.

Всього у конкурсі AES взяли участь *15 алгоритмів шифрування:*

1) CAST-256 (Entrust Technologies Inc.) – у алгоритмі не виявлено уразливостей, проте швидкість шифрування цього алгоритму невисока. Крім того, у нього високі вимоги до оперативної і енергонезалежної пам'яті.

2) Crypton (Future Systems Inc.) – алгоритм без явних недоліків, проте поступається за усіма характеристиками схожому на нього алгоритму Rijndael. Експерти конкурсу визнали, що у фіналі конкурсу Crypton однозначно програє алгоритму Rijndael, тому не вибрали його у другий раунд.

3) DEAL (R. Outerbridge, L. Knudsen) – має багато недоліків: наявність підмножин слабких ключів, уразливість до диференціального криптоаналізу, відсутність посилення при використанні 192-бітових ключів (порівняно з 128-бітовими).

4) DFC (Ecole Normale Superieurc) – має багато переваг, зокрема, дуже висока швидкість шифрування на 64-бітових платформах. При цьому алгоритм вельми повільно шифрує на останніх платформах, а також має класи слабких ключів.

5) E2 (NTT – Nippon Telegraph and Telephone Corporation) – аналогічно алгоритму Cast-256, в E2 не знайдено уразливостей, але вимоги до незалежної пам'яті дуже високі.

6) FROG (TecApro Internacional S.A.) – алгоритм з найбільш оригінальною структурою і з найбільшою кількістю недоліків: наявність різного роду уразливостей, низька швидкість шифрування і високі вимоги до ресурсів.

7) HPC (R. Schroeppel) – аналогічно алгоритму DFC, HPC дуже швидко шифрує на 64-бітових платформах, але вельми повільно на інших. Крім того, складна і повільна процедура розширення ключа обмежує можливе використання алгоритму, а найбільш складна, зі всіх представлених на конкурс алгоритмів, структура раунду ускладнює аналіз алгоритму і робить недоказовою відсутність закладок.

8) LOKI97 (L. Brown, J. Pieprzyk, J. Seberry) – має низьку швидкість шифрування, високі вимоги до ресурсів, невелику кількість уразливостей.

9) Magenta (Deutsche Telekom AG) схильний до атак методами лінійного і диференціального криптоаналізу, у нього повільна швидкість шифрування.

10) MARS (IBM) – в алгоритмі відсутні серйозні недоліки, за винятком низької швидкості шифрування на низці платформ, що не мають апаратної підтримки необхідних операцій. Алгоритм був дещо модифікований протягом першого раунду – змінений варіант вийшов у фінал конкурсу.

11) RC6 (RSA Laboratories) має дуже схожі на MARS проблеми з реалізацією на деяких платформах. Експерти зазначили це незначним недоліком – алгоритм вийшов у фінал конкурсу.

12) Rijndael (J. Daemen, V. Rijmen) – у цьому алгоритмі не виявлено недоліків, він вийшов у фінал конкурсу.

13) SAFER+ (Cylink Corporation) – алгоритм схильний до ряду атак і має низьку швидкість оброблення даних.

14) Serpent (R. Anderson, E. Biham, L. Knudsen) – виявлені деякі незначні недоліки, алгоритм вийшов у фінал конкурсу.

15) Twofish (B. Schneier, J. Kel-sey, D. Whiting, D. Wagner, C. Hall, N. Ferguson) – з недоліків експерти відзначили складність алгоритму, що ускладнює його аналіз, алгоритм вийшов у фінал конкурсу.

У результаті першого етапу конкурсу було вибрано 5 алгоритмів без явно виражених недоліків – це MARS, RC6, Rijndael, Serpent і Twofish. Почалося детальне вивчення саме цих алгоритмів (це називалося «другим етапом» або «фіналом» конкурсу AES), що продовжувалося ще більше року.

Результати виконаної аналітиками роботи щодо вивчення алгоритмів-фіналістів NIST сформулював у вигляді звіту. Цей звіт містить як результати аналізу алгоритмів, так і обґрунтування критеріїв, за якими виконувалася оцінка. На основі звіту можна коротко сформулювати порівняльні оцінки п’яти алгоритмів фіналістів конкурсу AES за основними критеріями (табл. 2.).

Таблиця 2

Порівняльні оцінки алгоритмів — фіналістів конкурсу AES

№	Критерій	Serpent	Twofish	MARS	RC6	Rijndael

1	Криптостійкість	+	+	+	+	+
2	Запас криптостійкості	++	++	++	+	+
3	Швидкість шифрування при програмній реалізації	-	+-	+-	+	+
4	Швидкість розширення ключа при програмній реалізації	+-	-	+-	+-	+
5	Смарт-карти з великим об'ємом ресурсів	+	+	-	+-	++
6	Смарт-карти з обмеженим об'ємом ресурсів	+-	+	-	+-	++
7	Апаратна реалізація (ПЛІС)	+	+	-	+-	+
8	Апаратна реалізація (спеціалізована мікросхема)	+	+-	-	-	+
9	Захист від атак за часом виконання і споживаною потужністю	+	+-	-	-	+
10	Захист від атак за споживаною потужністю на процедуру розширення ключа	+-	+-	+-	+-	-
11	Захист від атак за споживаною потужністю на реалізації в смарт-картах	+-	+	-	+-	+
12	Можливість розширення ключа «на льоту»	+	+	+-	+-	+-
13	Наявність варіантів реалізації (без втрат в сумісності)	+	+	+-	+-	+
14	Можливість паралельних обчислень	+-	+-	+-	+-	+

Щодо деяких рядків приведеної таблиці варто зауважити:

– Криптостійкість усіх алгоритмів-фіналістів виявилася достатньою – у процесі досліджень не було виявлено яких-небудь атак, що практично реалізовувалися, на повноцінних і повнораундових версіях алгоритмів. У цьому випадку криптоаналітики зазвичай досліджують варіанти алгоритмів з усіченою кількістю раундів, або з деякими внесеними змінами, що є незначними, але ослабляють алгоритм. Під запасом криптостійкості (Security Margin) експерти NIST мають на увазі співвідношення повної (передбаченої в специфікаціях алгоритмів) кількості раундів і максимального з тих варіантів, проти яких діють які-небудь криптоаналітичні атаки. Наприклад, за допомогою диференціально-лінійного криптоаналізу розкривається 11-раундовий Serpent, тоді як в оригінальному алгоритмі виконується 32 раунди. Експерти NIST у звіті попередили, що ця оцінка є досить поверхневою і не може бути значимою при виборі алгоритму переможця конкурсу. Проте, вони відзначили, що запас криптостійкості у Rijndael і RC6 є дещо нижчим ніж в інших алгоритмах-фіналістах.

– У пп. 5-8 приведена порівняльна оцінка можливості і ефективності реалізації алгоритмів у перерахованих пристроях.

– У пп. 9-11 мається на увазі наскільки операції, що виконуються конкретним алгоритмом, можуть бути схильні до аналізу вказаним методом. При цьому, враховувалося

те, що операції можуть бути модифіковані з метою ускладнення криптоаналізу за рахунок втрати у швидкості шифрування (наприклад, проблемне, в цьому сенсі, обертання на змінне число бітів може примусово виконуватися за рівне число тактів – тобто максимально можливе для даної операції; саме подібні заходи протидії атакам за часом виконання і споживаною потужністю рекомендує їх винахідник П. Кохер).

– З описів алгоритмів видно, що всі вони підтримують розширення ключа «на льоту» (тобто підключі можуть генеруватися безпосередньо в процесі шифрування – в міру необхідності), проте лише Serpent і Twofish підтримують таку можливість без будь-яких обмежень.

– Під наявністю варіантів реалізації (Implementation Flexibility) мається на увазі можливість по різному реалізовувати які-небудь операції алгоритму, оптимізуючи їх під конкретні цілі. Найбільш показовими в цьому сенсі є варіанти процедури розширення ключа алгоритму Twofish, що дозволяють оптимізувати реалізацію алгоритму в залежності, перш за все, від частоти зміни ключа.

Алгоритми-фіналісти, що не стали переможцями конкурсу:

Serpent

Алгоритм Serpent – це блоковий шифр, у якому блок даних розбивається на чотири підблоки по 32 біти (рис. 16). Сам алгоритм складається з 32 раундів: перед першим виконується початкова перестановка *(IP),* а після останнього – фінальна перестановка *(FP).*

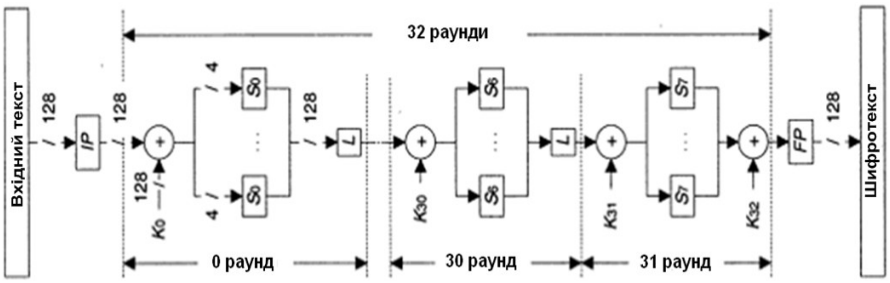

Рис. 16. Схема алгоритму SERPENT

Початкова перестановка визначається відповідно до рис. 2.1.6 – 0-й біт залишається на своєму місці, 32-й стає першим, 64-й другим і т.д. Фінальна перестановка є інверсною до початкової (рис. 19).

Функція раунду є досить простою:

1) Накладання 128-бітного ключа раунду побітовою логічною операцією XOR;

2) Таблична заміна: таблиці заміни є 4-бітовими перестановками (рис. 18) із властивостями стійкості до лінійного та диференціального криптоаналізу і тією властивістю, що порядок вихідних біт, як функції вхідних, повинен бути максимальний, тобто бути рівним 3.

0	32	64	96	1	33	65	97	2	34	66	98	3	35	67	99
4	36	68	100	5	37	69	101	6	38	70	102	7	39	71	103
8	40	72	104	9	41	73	105	10	42	74	106	11	43	75	107
12	44	76	108	13	45	77	109	14	46	78	110	15	47	79	111
16	48	80	112	17	49	81	113	18	50	82	114	19	51	83	115
20	52	84	116	21	53	85	117	22	54	86	118	23	55	87	119
24	56	88	120	25	57	89	121	26	58	90	122	27	59	91	123
28	60	92	124	29	61	93	125	30	62	94	126	31	63	95	127

Рис. 17. Початкова перестановка за алгоритмом SERPENT

Таблиця підстановок генерується з відомих і добре вивчених таблиць для алгоритму DES в ітераційному процесі, поки не будуть отримані бажані диференціальні й лінійні властивості. Таким чином, створюється 8 таблиць підстановок:

S_0	3	8	15	1	10	6	5	11	14	13	4	2	7	0	9	12
S_1	15	12	2	7	9	0	5	10	1	11	14	8	6	13	3	4
S_2	8	6	7	9	3	12	10	15	13	1	14	4	0	11	5	2
S_3	0	15	11	8	12	9	6	3	13	1	2	4	10	7	5	14
S_4	1	15	8	3	12	0	11	6	2	5	4	10	9	14	7	13
S_5	15	5	2	11	4	10	9	12	0	3	14	8	13	6	7	1
S_6	7	2	12	5	8	4	6	11	14	9	1	15	13	3	10	0
S_7	1	13	15	0	14	8	2	11	7	4	12	10	9	3	5	6

Рис. 18. Таблиці підстановки за алгоритмом SERPENT

Лінійне перетворення L задається таблицею, де біти перераховані від 0 до 127 (наприклад, вихідний 2 біт утворений 2, 9, 15, 30, 76, 84, 126 бітами, складеними за модулем 2). У кожному рядку описується 4 вихідних біти, які разом складають вхідні дані на одну таблицю замін у наступному раунді. Варто зазначити, що даний набір є таблицею $IP(L(FP(x)))$, де L і є лінійним перетворенням. Ця перестановка є зворотною до початкової $FP = IP^{-1}$ і задається таблицею, зображеною на рис. 19.

Щодо переваг алгоритму Serpent, варто відзначити: просту структуру алгоритму, що полегшує його аналіз з метою знаходження можливих уразливостей; можливість ефективно реалізувати апаратно і в умовах обмежених ресурсів; алгоритм легко модифікується з метою захисту від атак за часом виконання і споживаної потужності (проте за рахунок зниження швидкості).

0	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60
64	68	72	76	80	84	88	92	96	100	104	108	112	116	120	124
1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61
65	69	73	77	81	85	89	93	97	101	105	109	113	117	121	125
2	6	10	14	18	22	26	30	34	38	42	46	50	54	58	62
66	70	74	78	82	86	90	94	98	102	106	110	114	118	122	126
3	7	11	15	19	23	27	31	35	39	43	47	51	55	59	63
67	71	75	79	83	87	91	95	99	103	107	111	115	119	123	127

Рис. 19. Фінальна перестановка за алгоритмом SERPENT

Недоліки алгоритму: найповільніший з алгоритмів-фіналістів у програмних реалізаціях; процедури зашифрування і розшифрування абсолютно різні, тобто вимагають роздільної реалізації; розпаралелювання обчислень реалізується з обмеженнями.

Twofish

Алгоритм розроблений на основі алгоритмів Blowfish, SAFER та Square (рис. 20). Особливостями алгоритму є використання попередньо обчислюваних та залежних від ключа S-box'ів і складна схема розгортки підключення шифрування. Половина *n*-бітного ключа шифрування використовується як власне ключ шифрування, інша – для модифікації алгоритму (від неї залежать S-box'и). Twofish розбиває вхідний 128-бітний блок даних на чотири 32-бітних підблоки, над якими, після процедури вхідного відбілювання (Input Whitening), проводиться 16 раундів перетворень. Після останнього раунду виконується вихідне відбілювання (Output Whitening). Відбілювання істотно ускладнює завдання підбору ключа, оскільки криптоаналітик не може дізнатися, які дані потрапляють на вхід функції *F* першого раунду.

Функція g – основа алгоритму Twofish. На вхід функції подається 32-бітове число *X,* яке потім розбивається на чотири байти x0, x1, x2, x3. Кожен з отриманих байтів пропускається через свій S-box (слід зазначити, що S-box'и в алгоритмі не фіксовані, а залежать від ключа). Отримані чотири байти на виходах S-box'ів інтерпретуються як вектор з чотирма компонентами. Цей вектор множиться на фіксовану матрицю MDS (Maximum Distance Separable) розміром 4×4, причому обчислення проводяться у полі Галуа $GF(2^8)$ за модулем неприводного многочлена $x^8+x^6+x^5+x^3+1$. MDS матриця – це така матриця над кінцевим полем *K,* що якщо взяти її у якості матриці лінійного перетворення $f(x)=(MDS)$ з простору K^n у простір K^m , то будь-які два вектори з простору K^{n+m} виду $(x, f(x))$ будуть мати як мінімум $m + 1$ відмінностей у компонентах . Тобто набір векторів вигляду $(x, f(x))$ утворює код, що володіє властивістю максимального рознесення (таким кодом, наприклад, є код Ріда-Соломона). У Twofish властивість максимального рознесення матриці MDS означає, що загальна кількість змінних байт вектора *a* і вектора $b=(MDS)a$ не менше п'яти.

Іншими словами, будь-яка зміна тільки одного байта в *a* призводить до зміни всіх чотирьох байтів у *b*.

Криптоперетворення Адамара (Pseudo-Hadamar Transform, PHT) – оборотне перетворення бітового рядка довжиною $2n$. Рядок розбивається на дві частини *a* та *b* однакової довжини в *n* біт. Перетворення обчислюється таким чином: $a`=a+b \pmod{2^n}$ $b`=a+2b \pmod{2^n}$. Ця операція часто використовується для «розсіювання» коду (наприклад у шифрі SAFER). У Twofish це перетворення використовується при змішуванні результатів двох *g*-функцій ($n = 32$).

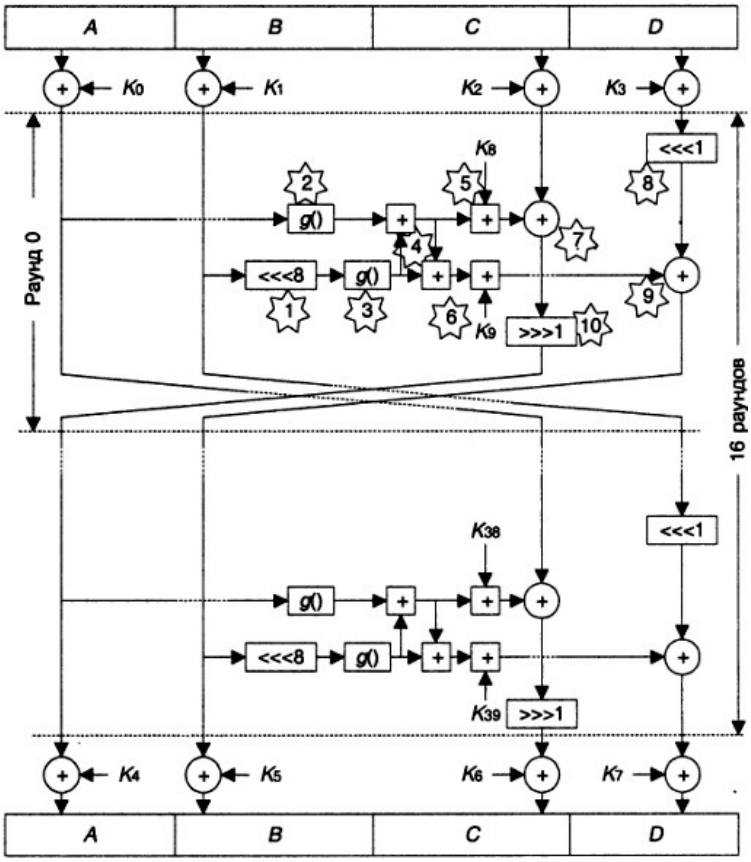

Рис. 20. Схема алгоритму Twofish

Циклічний зсув на 1 біт. У кожному раунді два правих 32-бітових блоки, які складаються XOR'ом з результатами функції *F,* додатково циклічно зсовуються на один біт. Третій блок зсовується до операції XOR, четвертий блок – після. Ці зсуви спеціально додані, щоб порушити вирівнювання за байтами, яке властиво S-box'ам та операції множення на MDS-матрицю. Проте шифр перестає бути повністю симетричним, так як при зашифруванні та розшифруванні зсуви слід здійснювати у протилежні сторони.

Генерація ключів. Twofish розрахований на роботу з ключами довжиною 128, 192 і 256 біт. З вихідного ключа генерується сорок 32-бітних підключів, перші вісім з яких використовуються тільки в операціях вхідного і вихідного відбілювання, а решта 32 – в раундах шифрування (по два підключі на раунд). Особливістю Twofish є те, що вихідний ключ використовується також і для зміни самого алгоритму шифрування, так як

використовуються у функції *g* S-box'и не фіксовані, а залежать від ключа. Для формування раундових підключів вихідний ключ *M* розбивається з перестановкою байт на два однакові блоки M_o та M_e. Потім за допомогою блоку M_o і функції *h* зашифровується значення $2\times i$, а за допомогою блоку M_e шифрується значення $2\times i+1$, де *i* – номер поточного раунду (0-15). Отримані зашифровані блоки змішуються криптоперетвореням Адамара, а потім використовуються як раундові підключі.

На рис. 20 цифрами 1-10 позначено:

1 – циклічний зсув вліво на 8 бітів вмісту підблоку *B;*

2 – оброблення підблоку *A* операцією *g();*

3 – оброблення підблоку *B* операцією *g();*

4 – підблок *B* накладається на *A* складанням за модулем 2^{32}, після чого аналогіч-ним чином підблок *A* накладається на *B;*

5 – фрагмент розширеного ключа K_{2r+8} (де *r* – номер поточного раунду почина-ючи з 0) складається з підблоком *A* за модулем 2^{32};

6 – аналогічно до попереднього кроку K_{2r+9} накладається на *B;*

7 – підблок *A* накладається на *C* операцією XOR;

8 – вміст підблоку *D* циклічно зсовується вліво на 1 біт;

9 – підблок *B* накладається на *D* операцією XOR;

10 – вміст під блоку *C* циклічно зсовується вправо на 1 біт.

Перевагами алгоритму Twofish є: можливість ефективної реалізації апаратно і в умовах обмежених ресурсів; процедури зашифрування і розшифрування в алгоритмі Twofish практично ідентичні; він є кращим з алгоритмів-фіналістів з точки зору підтримки розширення ключа «на льоту»; наявність декількох варіантів реалізації, що дозволяють оптимізувати алгоритм для конкретних використань. Недоліки алгоритму: складність структури алгоритму ускладнює його аналіз; складна і повільна процедура розширення ключа; відносно складно захищається від атак за часом виконання і споживаної потужності; розпаралелювання обчислень при шифруванні алгоритмом Twofish реалізовується з обмеження.

MARS

Відповідно до правил конкурсу AES протягом першого раунду конкурсу дозволялось вносити незначні зміни до алгоритмів – цим вдало скористались розробники алгоритму MARS, які змінили процедуру розширення ключа і цим знизили вимоги алгоритму до енергонезалежної та оперативної пам'яті.

MARS є блочним симетричним шифром (рис. 21), у якому розмір блоку при шифруванні 128 біт, розмір ключа може варіюватися від 128 до 448 біт включно (кратно 32 бітам). Розробники прагнули поєднати у своєму алгоритмі швидкість криптооброблення і стійкість шифру. У результаті вийшов один з найбільш криптостійких алгоритмів серед конкурсантів AES. Алгоритм унікальний тим, що використовував практично всі існуючі

технології, застосовувані в криптоалгоритмах, а саме: найпростіші операції (додавання, віднімання, XOR), підстановки з використанням таблиці замін, фіксований циклічний зсув, залежний від даних циклічний зсув, множення за модулем 2^{32} та ключове забілювання. Використання подвійного перемішування представляє ускладнює криптоаналіз (хоча деякі фахівці відносять це до недоліків алгоритму). У той же час, сьогодні не відомо будь-яких ефективних атак на цей алгоритм.

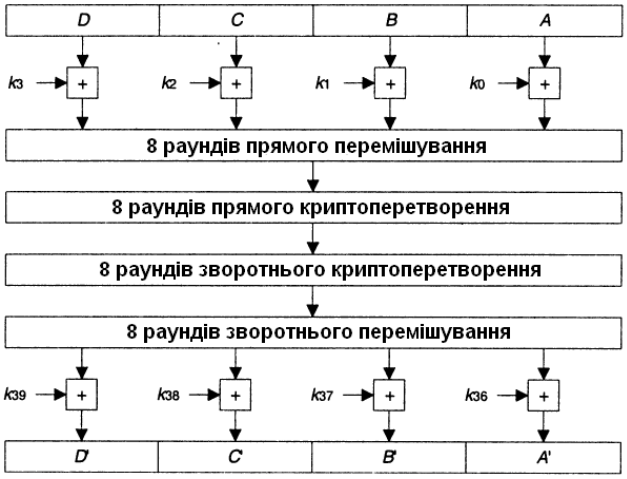

Рис. 21. Узагальнена схема алгоритму MARS

Третій та четвертий етапи (пряме та зворотнє криптоперетворення) реалізації алгоритму (рис. 21) називаються «криптографічним ядром» шифру MARS, $k_0 \ldots k_{39}$ – розширені ключі, а раунди прямого (зворотнього) перемішування та криптоперетворення містять досить складні процедури (ще один недолік алгоритму).

Беззаперечною перевагою алгоритму MARS є те, що процедури зашифрування і розшифрування є практично ідентичними. До недоліків слід віднести: виключно складну структуру алгоритму з раундами різних типів, що ускладнює як аналіз алгоритму, так і його реалізацію; виникнення проблем при програмній реалізації на тих платформах, які не підтримують 32-бітове множення і обертання на змінне число бітів; не можливість ефективної реалізації апаратно і в умовах обмежених ресурсів; складність захисту від атак за часом виконання і споживаною потужністю; гірше за інших фіналістів підтримує розширення ключів «на льоту»; розпаралелювання обчислень реалізується з обмеженнями.

RC6

Алгоритм RC6 – симетричний блоковий криптоалгоритм, похідний від свого попередника, алгоритму RC5 і запатентований компанією RSA Security. Варіант шифру RC6, заявлений на конкурс AES, підтримує блоки довжиною 128 біт і ключі довжиною 128, 192 і 256 біт, але сам алгоритм, як і RC5, може бути налаштований для підтримки більш широкого діапазону довжин як блоків, так і ключів (від 0 до 2040 біт). RC6 дуже схожий на RC5 за своєю структурою і також досить простий у реалізації. Аналогічно своєму попереднику, RC6 є повністю параметризованою сім'єю алгоритмів шифрування. Для специфікації алгоритму з

конкретними параметрами, прийнято позначення *RC6-w/r/b,* де w – довжина машинного слова в бітах, *r* – число раундів, а *b* – довжина ключа в байтах (0…255). Структура алгоритму представлена на рис. 22 – використовується 20 раундів перетворень, перед якими виконується часткове вхідне відбілювання, $K_0 ... K_{43}$ – фрагменти розширеного ключа, *f()* – функція, що виконує квадратичне перетворення $f(x)=x(2x+1) \bmod 2^{32}$.

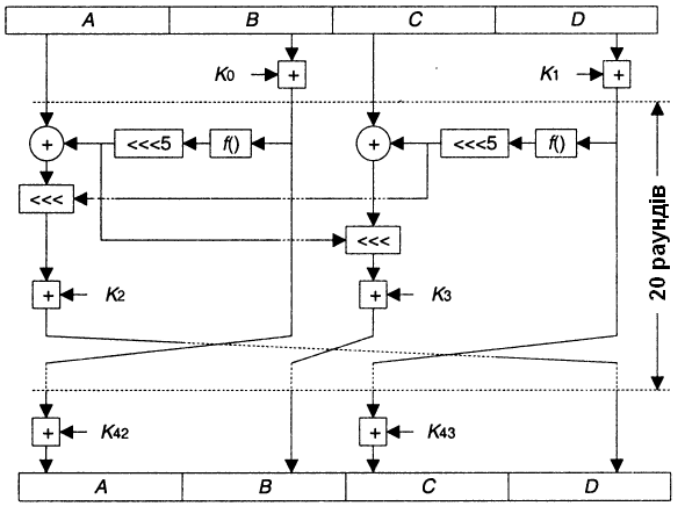

Рис. 22. Схема алгоритму RC6

Переваги алгоритму: проста структура алгоритму полегшує його аналіз. Крім того, алгоритм успадкував частину перетворень від алгоритму RC5, ретельно проаналізованого до конкурсу AES; найшвидший з алгоритмів-фіналістів на 32-бітових платформах; зашифрування і розшифрування в алгоритмі RC6 практично ідентичні. Недоліки: швидкість шифрування при програмній реалізації сильно залежить від того, чи підтримує платформа 32-бітове множення і обертання на змінне число бітів; складно реалізовується апаратно і в умовах обмежених ресурсів; досить складно захищається від атак за часом виконання і споживаної потужності; недостатньо повно підтримує розширення ключів «на льоту»; розпаралелювання обчислень реалізовується з обмеженнями.

У результаті переможцем конкурсу став алгоритм **Rijndael** – йому було привласнено назву AES. Вибір експертів не здається дивним – у табл. 2.1.1 видно, що практично за всіма характеристиками Rijndael, як мінімум, не поступається іншим алгоритмам-фіналістам. Що ж до алгоритмів Serpent, Twofish, MARS і RC6, то видно, що вони практично рівнозначні за сукупністю характеристик, за винятком алгоритму MARS, що має істотно більше недоліків, у тому числі алгоритм практично не реалізовується в умовах обмежених ресурсів.

Rijndael (AES)

У принципі, алгоритм, запропонований авторами, та стандарт AES не одне і те ж – алгоритм Rijndael підтримує широкий діапазон розміру блоку та ключа, а AES має фіксовану довжину у 128 біт, а розмір ключа може приймати значення 128, 192 або 256 біт, у той час як Rijndael підтримує розмірність блоку та ключа із кроком 32 біт у діапазоні від 128 до 256. Через фіксований розмір блоку AES оперує із масивом 4×4 байт, що називається станом

(версії алгоритму із більшим розміром блоку мають додаткові колонки). Для ключа у 128 біт алгоритм має 10 раундів, у яких послідовно виконуються операції: *SubBytes(), ShiftRows(), MixColumns()* (у десятому раунді ця операція пропускається) та *AddRoundKey()*.

SubBytes(). У процедурі *SubBytes()* кожен байт в масиві *State* замінюється відповідним елементом у фіксованій 8-бітній таблиці пошуку (рис. 22). Процедура *SubBytes()* обробляє кожен байт стану незалежно, проводячи нелінійну заміну байтів використовуючи таблицю замін (S-box).

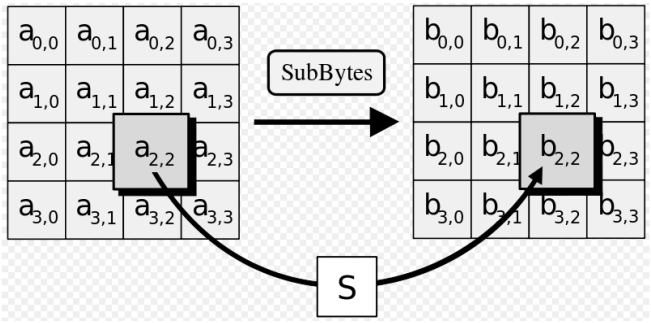

Рис. 22. Схема процедури *SubBytes()*

Така операція забезпечує нелінійність алгоритму шифрування. Побудова S-box складається з двох кроків. По-перше, проводиться отримання зворотного числа у полі Галуа $GF(2^8)$. По-друге, до кожного байту b, з яких складається S-box, застосовується така операція: $B'_i = b_i \oplus b_{(i+4)\bmod 8} \oplus b_{(i+5)\bmod 8} \oplus b_{(i+6)\bmod 8} \oplus b_{(i+7)\bmod 8} \oplus c_i$, де $0 \le i < 8$, і де b_i є i-ий біт b, а c_i – i-ий біт константи $c = 63_{16} = 99_{10} = 01100011_2$.

Таким чином, забезпечується захист від атак, заснованих на простих алгебраїчних властивостях. S-box можна відобразити таблицею простої підстановки (рис. 23):

S-box

\	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Рис. 23. Таблиця S-box

Наприклад, на вході 19 на виході отримаємо d4. Фактично, S-box – це звичайний шифр простої підстановки.

ShiftRows(). Процедура *ShiftRows()* працює з рядками таблиці State. При цій трансформації рядка відбувається циклічний зсув на r байт по горизонталі, залежно від номера рядка (рис. 24). Для нульового рядка $r = 0$, для першого – $r = 1$ і т.д. Таким чином, кожна колонка вихідного стану після застосування процедури *ShiftRows()* складається з байтів кожної колонки початкового стану. Для алгоритму Rijndael патерн зсуву рядків для 128- і 192-бітних рядків однаковий. Однак, у випадку блоку розміром 256 біт, патерн відрізняється від попередніх тим, що 2, 3, і 4-й рядки зміщуються на 1, 3, і 4 байти відповідно. Фактично *ShiftRows()* – це проста перестановка байт таблиці 4×4 State.

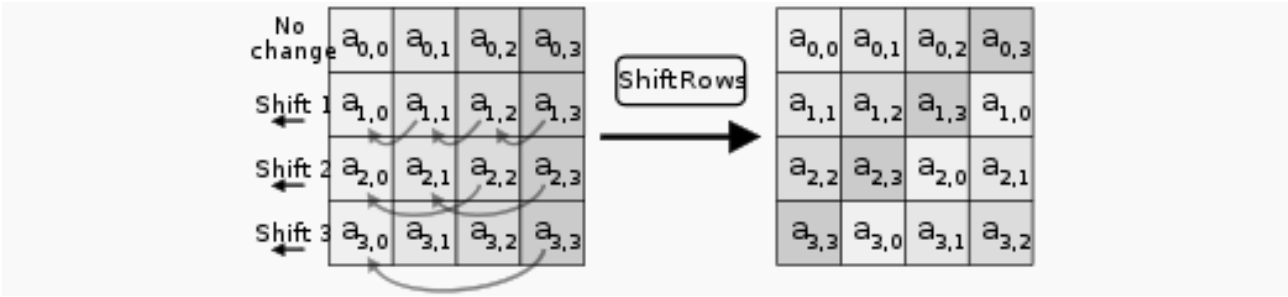

Рис. 24. Процедура *ShiftRows()*

MixColumns(). У процедурі *MixColumns()* чотири байти кожної колонки State змішуються, використовуючи для цього зворотну лінійну трансформацію (рис. 25). *MixColumns()* опрацьовує стан по колонках, трактуючи кожну з них як поліном четвертого степеня. Над цими поліномами виконується множення у $GF(2^8)$ за модулем x^4+1 на фіксований многочлен $c(x)=3x^3+x^2+x+2$. Разом з *ShiftRows()*, *MixColumns()* вносить дифузію в шифр.

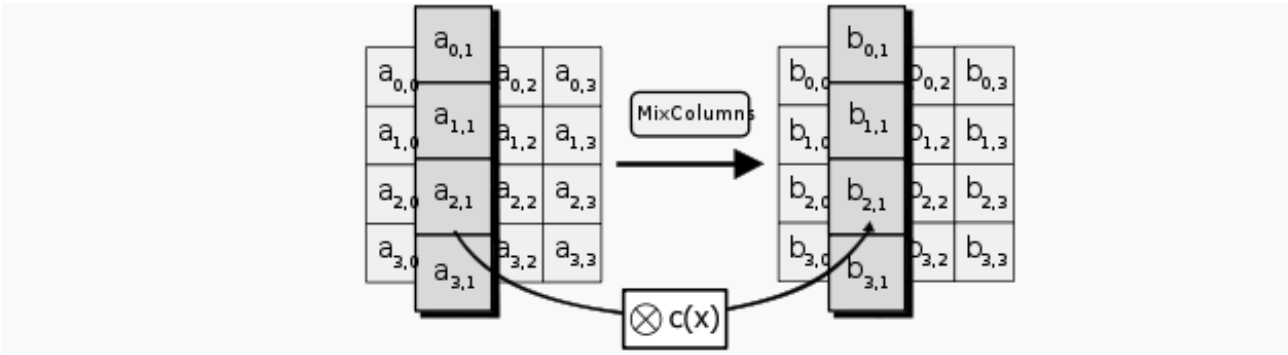

Рис. 25. Процедура *MixColumns()*

Під час операції *MixColumns(),* кожен стовпчик множиться на матрицю, яка для 128-бітного ключа має вигляд:

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}.$$

AddRoundKey(). У процедурі *AddRoundKey()* кожен байт стану об'єднується з *RoundKey,* використовуючи операцію XOR (рис. 26):

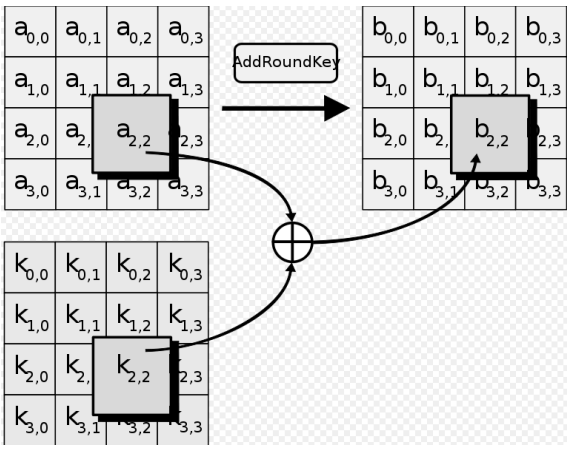

Рис. 26. Процедура *AddRoundKey()*

Конкурс NESSIE

Європейський конкурс криптоалгоритмів *NESSIE (New European Schemes for Signatures, Integrity & Encryptions)* стартував трохи пізніше за конкурс AES – у лютому 2000 р. Як видно з назви, цілі конкурсу NESSIE були помітно ширшими, ніж в конкурсу AES. У рамках конкурсу NESSIE розглядалися алгоритми таких категорій:

1) блокове симетричне шифрування (на конкурс прийнято 17 алгоритмів);

2) потокове шифрування (6 алгоритмів);

3) обчислення коду автентифікації (MAC) повідомлень (2 алгоритми);

4) гешування (1 алгоритм);

5) асиметричне шифрування (5 алгоритмів);

6) ЕЦП (7 алгоритмів);

7) ідентифікація (1 алгоритм).

Як і на конкурсі AES, алгоритми-учасники конкурсу були прислані практично зі всього світу. Причому абсолютним лідером за кількістю розглянутих на конкурсі алгоритмів була Японія – з 39 учасників конкурсу в Японії було розроблено 8. На відміну від конкурсу AES, єдиною експертною організацією якого був інститут NIST, організатором конкурсу NESSIE був інтернаціональний консорціум з організацій, відомих своїми дослідженнями в області криптології: Католицький Університет (м. Лювен, Бельгія) – координатор проекту; вищий учбовий заклад Ecole Normale Superieure (м. Париж, Франція); університет Royal Holloway (м. Лондон, Великобританія); корпорація Siemens AG (Німеччина); Технологічний Інститут Technion (м. Хайфа, Ізраїль); Університет Берген (Норвегія).

Ще одна принципова відмінність NESSIE (відносно алгоритмів блокового шифрування) від конкурсу AES полягала у тому, що не був встановлений конкретний розмір блоку даних, тому в конкурсі розглядалися 64-, 128-, 160- та 256-бітові блокові шифри. Ще одна аналогія з конкурсом AES – два раунди конкурсу. Причому їх призначення повністю аналогічно конкурсу AES: у першому раунді конкурсу NESSIE розглядались усі алгоритми, з яких в другий раунд були вибрані ті з них, у яких не було явно виражених недоліків. Відповідно, у другому раунді з фіналістів були вибрані кращі:

– *блокові шифри:* MISTY1 (Mitsubishi Electric Corp., Японія), Camellia (Nippon Telegraph and Telephone Corp., Японія та Mitsubishi Electric Corp., Японія), SHACAL-2 (Gemplus, Франція) та переможець конкурсу AES – шифр Rijndael;

– *асиметричні шифри:* ACE Encrypt (Науково-дослідна лабораторія IBM, Швейцарія), PSEC-KEM (Nippon Telegraph and Telephone Corp., Японія), RSA-KEM* (проект ISO/IEC 18033-2);

– *MAC алгоритми і геш-функції:* Two-Track-MAC (K.U. Leuven, Бельгія, Debis AG, Німеччина), UMAC (Intel Corp., США, університет Невади, США, Науково-дослідна лабораторія IBM, США, Technion, Израиль и университет Калифорнии в Дэвисе, США), CBC-MAC* (ISO/IEC 9797-1), HMAC* (ISO/IEC 9797-1), Whirlpool (Scopus Tecnologia S.A., Бразилія та K.U. Leuven, Бельгія), SHA-256*, SHA-384* та SHA-512* (USA FIPS 180-2).

– *алгоритми цифрового підпису:* ECDSA (Certicom Corp., США and Certicom Corp., Канада), RSA-PSS (лаборатории RSA, США), SFLASH (Schlumberger, Франція).

– *методи ідентифікації:* GPS (Ecole Normale Supérieure, Франція та Télécom and La Poste,Франція).

Критерії для розробки сучасних симетричних криптоалгоритмів

Сучасний алгоритм симетричного шифрування повинен:

– оперувати даними у великих блоках, переважно розміром 16 або 32 біти, мати розмір блоку 64 або 128 біт, мати масштабований ключ до 256 біт;

– використовувати прості операції, які ефективні на мікропроцесорах, тобто XOR, додавання, табличні підстановки, складання за модулем (не припустиме використання зсувів змінної довжини, побітових перестановок або умовних переходів);

– повинна бути можливість реалізації алгоритму на 8-бітовому процесорі з мінімальними вимогами до пам’яті;

– використовувати заздалегідь обчислені підключі;

– складатися зі змінного числа ітерацій (для застосунків з малою довжиною ключа недоцільно застосовувати велике число ітерацій для протистояння диференціальним та іншим атакам);

– за можливістю, не мати слабких ключів (якщо це неможливо, то кількість слабких ключів має бути апріорі відомою і мінімальною, щоб зменшити вірогідність випадкового вибору одного з них);

– задіювати підключі, які є одностороннім гешем ключа (це дає можливість використовувати великі парольні фрази у якості ключа без загрози безпеці);

– не мати лінійних структур, які зменшують комплексність і не забезпечують достатній пошук;

– використовувати просту для розуміння розробку (це дає можливість аналізу і зменшує закритість алгоритму).

Асиметрична криптографія

Як зазначалось раніше, розподіл ключів – це одна з актуальних проблем у сучасній криптографії. Одним з ефективних методів розподілу ключів шифрування є використання криптографічної схеми з відкритим ключем. Яскравим прикладом такої схеми є *протокол Діфі-Хелмана (Diffie-Hellman)* та *цифровий конверт.* Схема Діфі-Хелмана дозволяє двом легітимним користувачам обмінятися секретним ключем відкритим каналом без попередньої зустрічі. Схема цифрового конверту (digital envelope) передбачає такі дії:

a) генерація сесійного (одноразового) ключа;

b) зашифровування повідомлення сесійним секретним ключем;

c) зашифровування відкритого ключа отримувача – це і буде цифровим конвертом;

d) зашифроване повідомлення та цифровий конверт передаються легітимному користувачеві;

e) 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 криптооброблення (для прикладу, найшвидша реалізація одного з найвідоміших асиметричних алгоритмів RSA є повільнішою за типовий симетричний алгоритм мінімум на три порядки).

Загалом, *асиметричні криптосистеми* – ефективні системи криптографічного захисту даних, у яких для зашифровування даних використовується один ключ, а для розшифровування – інший ключ (звідси і назва – асиметричні). Перший ключ є *відкритим (Public Key)* 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 (Secret Key).* 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. 27). Необхідність відправникові й одержувачеві погоджувати таємний ключ спеціальним захищеним каналом цілком відпала.

Прикладами криптосистем з відкритим ключем є *система Ель-Гамаля* (названа на честь автора, Т. Ельгамаля), *RSA* (названа на честь винахідників: Р. Рівеста, А. Шаміра і Л. Адлмана), згадана раніше *система Діфі-Хелмана* та *DSA* (Digital Signature Algorithm, винайдений Д. Кравіцом).

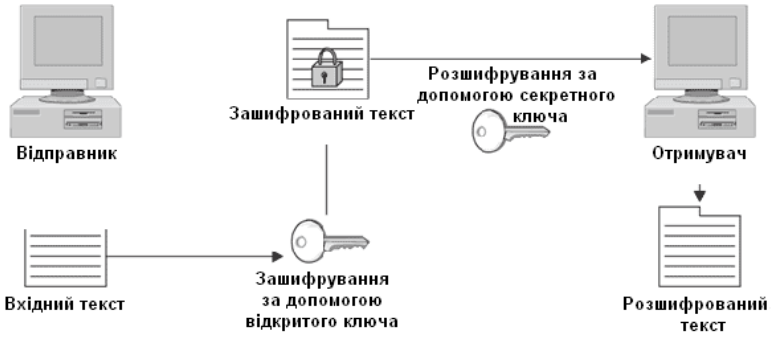

Рис. 27. Типова схема асиметричної криптографії

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 нездійсненно. Зокрема, таке може статися за необхідності використання мережі Інтернет як середовища передачі даних і, одночасно, необхідність 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 помилкового зв’язку, а також застосовувати їх замість легального користувача, чий відкритий ключ був скомпрометований. На практиці при застосуванні асиметричного алгоритму шифрування у 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 математичних задачах, які на сьогодні є важкообчислювальними навіть для методу «грубої сили»:*

- дискретне логарифмуванню в кінцевих полях;
- знаходження коренів великих чисел;
- факторизація великих чисел.

Оскільки сьогодні не існує ефективних алгоритмів розв’язання цих задач або їх розв’язок вимагає залучення великих обчислювальних ресурсів (чи тимчасових витрат), ці задачі знайшли широке застосування у побудові асиметричних алгоритмів. Проте, стійкість,

що базується на гіпотетичній неможливості розв'язання певних математичних задач, не є абсолютною – це відкриває «широке поле» для наукових досліджень у цьому напрямі (С.Г.).

Основні параметри шифрів

Стійкість шифру. Певні шифри вважаються досконалими у тому розумінні, що перехоплення супротивником криптограми не зменшує невизначеності у можливому виборі відкритого тексту. Такі шифри належать до класу теоретично стійких шифрів, стійкість яких базується на доведених теоремах про неможливість розкрити ключ. Але не практиці широко використовуються ті шифри, для яких зазначена невизначеність після перехоплення криптограми повністю зникає. Інакше кажучи, стає відомо, що криптограму отримано при шифруванні лише одного відкритого тексту, але якого саме – невідомо. Рівень стійкості таких криптосистем оцінюється витратами часу, зусиль і потужністю обчислювальних засобів, необхідних для одержання цього єдиного відкритого тексту. При надвеликих витратах і незначній імовірності успіху дешифрування суттєво змінилось визначення *практичної стійкості* алгоритмів з відкритим ключем, зокрема з`явилося поняття *довідної стійкості.* Тепер криптологам немає потреби вдаватися у довгі інтуїтивні обґрунтування безпеки шифрів з відкритим ключем, бо вони зводять їх злам до розв`язання добре вивчених складних математичних задач, які даремно намагалися розв`язати багато математиків. Прикладом шифру з довідною стійкістю можуть слугувати криптосистеми RSA або Діфі-Хелмана, що базуються на складнощах факторизації великих чисел і дискретного логарифмування відповідно. Недолік шифрів з довідною стійкістю полягає у неможливості оперативно допрацювати криптоалгоритм у разі потреби, тобто їх жорсткість. Підвищити стійкість можна тільки за рахунок збільшення розмірності математичної задачі, покладеної в основу криптосистеми, або заміни самої задачі. Зазвичай, це викликає цілу низку додаткових змін у шифрувальній або суміжній апаратурі.

Статистичні характеристики шифру. Як відомо, до криптоалгоритмів висуваються такі основні вимоги: відсутність статистичної залежності між текстом і криптограмою; за статистичними властивостями криптограма не може різнитися від істинно ВП; зміна будь-якого біта ключа шифрування при незмінному відкритому тексті має змінювати принаймні 50% бітів криптограми (для симетричних алгоритмів); зміна будь-якого біта відкритого тексту при незмінному ключі шифрування має викликати принаймні 50% бітів криптограми (для блокових алгоритмів). Процес та методи оцінки рівня випадковості описано у наступному підрозділі цієї теми.

Складність зламу шифру. Сучасних криптографів насамперед цікавлять криптосистеми, які важко зламати доступними обчислювальними засобами (нині або в майбутньому). Складність зламу шифру поєднує у собі обсяг інформації для розкриття криптоаналітиком алгоритму шифрування, час на опрацювання даних, вимоги щодо швидкодії та обсягу пам`яті у засобах комп`ютерної техніки.

Складність виконання операцій шифрування. Спосіб, в який здійснюються операції зашифрування/розшифрування, має бути якомога простішим. Якщо проводити операції вручну, то складність процесу обумовлює появу помилок та чималі витрати часу. При використанні ж шифрувальної апаратури набувають актуальності простота і технологічність її реалізації, прийнятна вартість, забезпечення належної швидкості зашифрування та розшифрування.

Зростання кількості помилок. У деяких шифрів помилка в одній букві, допущена при шифруванні, призводить до великої кількості помилок у розшифрованому тексті. Такі помилки розростаються через операції розшифрування, стають причиною значної втрати інформації, і часто потім потрібно повторно шифрувати текст і передавати нову криптограму. Тож, при виборі шифру слід намагатися мінімізувати, або взагалі усунути зростання помилок.

Перешкодостійкість шифру. Під впливом перешкод у лініях зв`язку текст криптограми може спотворюватися, що призводить до появи неабияких перекручень у розшифрованому тексті, а нерідко й до втрати його сенсу. Властивість шифру протидіяти розростанню помилок при розшифруванні криптограм називається їх *перешкодостійкістю.*

Імітостійкість шифру. Активні імітодії порушників у каналі зв`язку – це спроби нав`язати абонентам мережі (легітимним користувачам) неправдиву інформацію шляхом викривлення криптограми у каналі зв`язку або замінити справжню криптограму на раніше переданий шифрований текст. Шифри із здатністю протистояти таким спробам називають *імітостійкими.*

Збільшення обсягу повідомлення. Деякі шифри мають властивість значно нарощувати обсяг повідомлень у процесі шифрування. Наприклад, цей небажаний ефект спостерігається у намаганнях приховати статистику повторюваності букв відкритого тексту введенням у криптограму певних допоміжних символів або при рандомізації відкритого повідомлення (застосування до нього певного пропорційного коду).

Сфери застосування. Стандартний (типовий) алгоритм шифрування повинен застосовуватися для розв’язання декількох задач: 1) шифрування даних (алгоритм має бути ефективним при шифруванні файлів, даних або великого потоку даних); 2) створення ВП (алгоритм має бути ефективним при створенні певної кількості випадкових біт); 3) гешування (алгоритм повинен ефективно перетворюватися в односторонню геш-функцію).

Теоретичні основи оцінки статистичних властивостей ГВП (ГПВП)

Застосування ВП (ПВП) у криптографії є досить важливим, так як вони можуть забезпечити *необхідний рівень стійкості при формуванні ключа шифрування* (а від стійкості ключа, у більшості випадків, і залежить стійкість усієї криптосистеми). Крім того, як видно із параметрів шифрів, *типовий алгоритм шифрування на виході має давати ПВП з високим рівнем випадковості.* Взагалі, *ВП* – це така послідовність чисел, для якої неможливо передбачити наступне число, навіть якщо відомі попередні, а *ПВП* – це послідовність чисел,

яка має властивості ВП, проте кожне наступне число обчислюється за певною формулою чи законом (псевдовипадкова двійкова (бінарна) послідовність є частковим випадком ПВП, хоча бувають й інші, наприклад, трійкові (тритові) тощо). Для отримання ВП та ПВП використовують обчислювальний або фізичний пристрій, спроектований для генерації послідовності номерів чи символів, які не відповідають будь-якому шаблону – ГВП. Деякі науковці вважають, що немає істино випадкових генераторів, а є лише ГПВП, відповідно і результатом їх роботи є різного роду ПВП, а не ВП. Хоча ПВП на перший погляд може здатися позбавленою закономірностей, проте будь-який ГПВП з кінцевим числом внутрішніх станів повториться після дуже довгої послідовності чисел (що доводиться за допомогою принципу Діріхле). Основним завданням розробників таких генераторів є забезпечення якомога більшого періоду повторюваності.

Внаслідок швидкого розвитку методів статистичного моделювання і криптографії, галузь застосування ГВП істотно розширилася. Можливість реалізації ГВП для зазначених галузей 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. Як уже зазначалось, ГВП використовуються в існуючих криптосистемах для генерації ключової інформації і визначення ряду параметрів криптосистем. Відповідно до зазначеного принципу Керкхоффса, стійкість криптографічного алгоритму не має залежати від архітектури алгоритму, а лиш від ключів шифрування. Іншими словами, при оцінюванні надійності шифрування необхідно вважати, що супротивник знає все про систему шифрування, яка 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).

Усі послідовності, породжувані ГВП (ГПВП) для криптографічних цілей, підлягають обов'язковому тестуванню. *Тестування ПВП* – це сукупність методів та засобів визначення міри близькості заданої ПВП до ВП. У якості критерію зазвичай виступає наявність рівномірного розподілу, великого періоду, рівної частоти появи однакових підрядків тощо. Існують такі *методи тестування ПВП:*

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 (вплив людського чинника).

2) Статистичні тести. На відміну від графічних, статистичні тести видають чисельну характеристику ПВП і дозволяють однозначно сказати, чи пройдений конкретний

тест, чи ні. Сьогодні найбільш відомими і використовуваними є такі статистичні тести: тести Д. Кнута, DIEHARD, CRYPT-X, NIST STS, FIPS та ін.

Вимоги до генерування ПВП

Одне з перших формулювань деяких основних правил для статистичних властивостей періодичних ПВП була представлена С. Голомбом. Три основних правила отримали популярність як постулати Голомба: 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 одна відносно одної на деяке значення d. Тоді для кожного d ($0 \le d \le pl$) можна підрахувати кількість узгоджень між цими двома послідовностями Ad і кількість неузгодженостей Dd. Коефіцієнт автокореляції для кожного d визначається співвідношенням $(Ad - Dd)/p$, а функція автокореляції приймає різні значення у міру того, як d проходить всі допустимі значення. Тоді для будь-якої послідовності, що задовольняє 3-му правилу, автокореляційна функція повинна приймати лише два значення.

Контрольні запитання

1) Розв'язання яких основних задач покладено на криптографію? Які розділи криптографії Ви знаєте?

2) Сформулюйте вимоги до сучасних криптосистем. Назвіть і поясніть основні принципи криптографії.

3) Які шифри називають блоковими і як їх можна класифікувати?

4) У чому полягають особливості потокових шифрів і які їх види Ви знаєте?

5) Дайте характеристику алгоритмам-фіналістам конкурсу AES.

6) З якою метою проводився конкурс NESSIE і які його результати?

7) Які існують критерії для розробки сучасних криптосистем?

8) Принципи роботи криптосистем з відкритим ключем (їх структурні особливості).

9) Які Ви знаєте параметри шифрів? Охарактеризуйте кожен з них.

10) Роль ГВП (ГПВП) у сучасній криптографії.

Тема 7. Особливості побудови захищених систем передачі даних на основі бездротових технологій

Основи безпеки бездротових систем передачі даних. Сьогодні надзвичайно важливу роль відіграє швидке та безпечне передавання інформації. З огляду на це, на розробку таких методів, способів витрачаються дуже великі кошти і, з точки зору програмування, вони становлять собою досить складні програмні комплекси, що розроблялись, як правило, цілими групами спеціалістів. Створення такої захищеної мережі – це доволі трудомістке завдання, оскільки мережа орієнтується на користувачів, які мають передавати інформацію з обмеженим доступом. Така інформація як правило відіграє важливу стратегічну роль у роботі підприємства і не повинна бути перехопленою сторонніми користувачами.

Останніми роками напрям бездротових технологій передавання даних та віддаленого доступу зазнав бурхливого розвитку. Це пов'язано з поширенням ноутбуків та нетбуків, систем пошукового виклику (так званих пейджерів), появою систем класу «персональний секретар» (Personal Digital Assistant, PDA), а також розширенням функціональних можливостей стільникових телефонів (рис. 28). Такі системи мають забезпечити ділове планування, розрахунок часу, зберігання документів та підтримку зв'язку з віддаленими станціями. Девізом цих систем стало «anytime & anywhere», тобто надання послуг зв'язку незалежно від місця та часу. Крім того, бездротові канали зв'язку є актуальними там, де неможливе або надто дороге прокладання кабельних ліній.

Wi-Fi (Wireless Fidelity, бездротова точність) – це технологія бездротового обміну даними, що відноситься до групи стандартів IEEE 802.11. Сьогодні ця технологія є дуже популярною в усьому світі. Для прикладу, якщо ноутбук і подивитися на кількість Wi-Fi мереж у будь-якому мікрорайоні Києва (чи іншого великого міста), то їх там буде не дві і не три, а набагато більше. На жаль, таке поширення у маси призводить до того, що багато людей ставлять у себе бездротове обладнання, навіть не розібравшись у налаштуваннях. Наслідком некоректного налаштування обладнання може стати можливість отримання НСД до бездротової мережі і, як наслідок, до даних, що у ній циркулюють.

Крім групи стандартів IEEE 802.11 a/b/g/n (Wireless Networks, бездротові мережі) на сьогоднішній день існують ще такі групи:

- 802.1 (Internetworking, об'єднання мереж);
- 802.2 (Logical Link Control, LLC, керування логічною передачею даних);
- 802.3 (Ethernet з методом доступу CSMA/CD);
- 802.4 (Token Bus LAN, локальні мережі з методом доступу Token Bus);
- 802.5 (Token Ring LAN, локальні мережі з методом доступу Token Ring);
- 802.6 (Metropolitan Area Network, MAN, мережі мегаполісів);

– 802.7 (Broadband Technical Advisory Group, технічна консультаційна група щодо широкополосної передачі даних);

– 802.8 (Fiber Optic Technical Advisory Group, технічна консультаційна група щодо волоконно-оптичних мереж);

– 802.9 (Integrated Voice and data Networks, інтегровані мережі передачі голосу і даних);

– 802.10 (Network Security, мережева безпека);

– 802.12 (Demand Priority Access LAN, l00VG-AnyLAN, локальні мережі з методом доступу за вимогою з пріоритетами);

– 802.14 (Cable modems, кабельні модеми);

– 802.15 (Wireless PAN, бездротові персональні мережі);

– 802.16 (WiMAX, бездротові мережі міського масштабу);

– 802.20 (Mobile Broadband Wireless Access, MBWA, бездротовий широкосмуговий мобільний доступ) та ін.

Рис. 28. Комунікаційні пристрої у радіусі дії Wi-Fi мережі

Стандарти технології IEEE 802.11 – це серія стандартів, прийнятих інститутом IEEE, які визначають взаємодію бездротових комп'ютерних мереж. Вони, у свою чергу, диференціюються таким чином:

– 802.11 – початковий (базовий) стандарт бездротових локальних мереж (прийнятий у 1997 р.), заснований на бездротовій передачі даних у діапазоні 2,4 Ггц. Підтримує обмін даними зі швидкістю до 1-2 Мбіт/с.

– 802.11a – стандарт бездротових локальних мереж, заснований на бездротовій передачі даних у діапазоні 5 ГГц. Діапазон роздільний на три непересічні канали. Максимальна швидкість обміну даними складає 54 Мбіт/с, при цьому доступні також швидкості 48, 36, 24, 18, 12, 9 і 6 Мбіт/с.

– 802.11b – стандарт бездротових локальних мереж, заснований на бездротовій передачі даних у діапазоні 2,4 ГГц. У всьому діапазоні існує три непересічні канали, тобто на одній території, не впливаючи один на одного, можуть працювати три різні бездротові мережі. У стандарті передбачено два типи модуляції – DSSS (Direct Sequence Spread Spectrum, розширення спектру методом прямої послідовності) та FHSS (Frequency Hopping

Spectrum Spreading, швидка псевдовипадкова перебудова робочої частоти). Максимальна швидкість роботи складає 11 Мбіт/с, при цьому доступні також швидкості 5,5, 2 і 1 Мбіт/с.

– 802.11g – стандарт бездротових локальних мереж, заснований на бездротовій передачі даних у діапазоні 2,4 ГГц зі швидкістю 54 Мбіт/с. Діапазон, аналогічно попередньому, розділений на три непересічні канали. Для збільшення швидкості обміну даними при ширині каналу, схожій з 802.11b, застосовані методи модуляції OFDM (Ortogonal Frequency Division Multiplexing, метод модуляції з ортогональним частотним мультиплексуванням) та PBCC (Packet Binary Convolutional Coding, метод двійкового пакетного згорткового кодування).

– 802.11n – стандарт бездротових локальних мереж останнього покоління, заснований на бездротовій передачі даних в діапазоні 2,4 ГГц, швидкість – 600 Мбіт/с.

– 802.11e (QoS) – додатковий стандарт, що дозволяє забезпечити гарантовану якість обміну даними шляхом перестановки пріоритетів різних пакетів; необхідний для роботи таких потокових сервісів як VoIP або IP-TV.

– 802.11i (WPA2) – стандарт, що знімає недоліки в області безпеки попередніх стандартів. Цей стандарт вирішує проблеми захисту даних канального рівня і дозволяє створювати безпечні бездротові мережі практично будь-якого масштабу.

Крім цих типів є спеціальні модифікації від різних виробників обладнання. Зазвичай вони називаються як назва стандарту із знаком «плюс», наприклад, 801.11b+, 801.11g+. При використанні в мережі точки доступу цього виробника і виключно обладнання цього ж виробника межа пропускної здатності може бути значно збільшена.

Методи шифрування у бездротових мережах

1) Протокол WEP. Цей протокол заснований на потоковому шифрі RC4. На сьогодні час в шифрі RC4 були знайдені численні уразливості, тому, з точки зору безпеки, використовувати WEP не рекомендується. WEP шифрування може бути статичним або динамічним. При статичному WEP-шифруванні ключ не змінюється. При динамічному, після певного періоду, відбувається зміна ключа шифрування.

Існує два стандартні варіанти WEP: а) з довжиною ключа 128 біт, при цьому 104 біта є ключовими і 24 біта в ініціалізаційному векторі (IV). Також, цей варіант ще іноді називають 104-бітним WEP; б) з довжиною ключа 64 біт, при цьому 40 біт є ключовими і 24 біта в IV (40-бітний WEP). Існують ще варіанти з довжиною 152 біта і 256 біт, але просте збільшення ключа у випадку WEP є тривіальною операцією, що не додає стійкості. Вектор ініціалізації (IV) застосовується для підвищення секретності шляхом рандомізації додаткової частини ключа (рис. 29). Проте, злом такого захисту не є складною задачею навіть для не професіоналів – відповідні утиліти є загальнодоступними і їх можна вільно завантажити з Інтернет. Основним слабким місцем і є IV, оскільки мова йде про 24 біти (2^{24} комбінацій), далі ключ повторюється. Завдання хакера зводиться до пошуку цих повторів (15-45 хвилин

для ключа 40 біт), а далі за лічені секунди зламується інша частина ключа і він може підключатися до мережі як звичайний легітимний користувач.

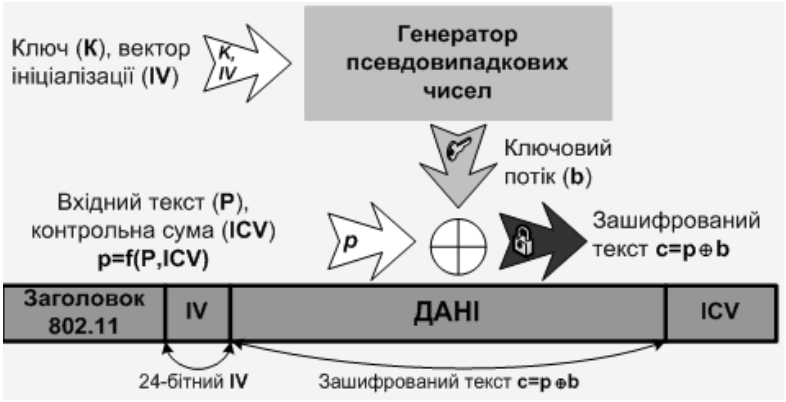

Рис. 29. Схема формування ключа у протоколі WEP

2) Протокол WPA. Цей протокол є тимчасовим стандартом, про який домовилися виробники устаткування, поки не набув чинності стандарт IEEE 802.11i. По суті, WPA = 802.1X + EAP + TKIP + MIC, де: EAP – протокол розширеної автентифікації, TKIP – протокол інтеграції тимчасового ключа (безпосередньо протокол шифрування), MIC – технологія перевірки цілісності повідомлень. Автентифікація може реалізуватись за допомогою RADIUS сервера (WPA-Enterprise) та за допомогою попередньо встановленого ключа (WPA-PSK).

Згаданий протокол TKIP використовує той же шифр RC4 що і WEP, але тепер IV має довжину 48 біт, крім цього доданий протокол Michael для перевірки цілісності повідомлень (MIC). Якщо протягом хвилини буде надіслано понад два пакети, що не пройшли перевірку, то бездротовий клієнт буде заблокований на одну хвилину. Тепер RC4 вже використовується не у «чистому вигляді» як у WEP, містить заходи проти відомих атак на цей шифр. Однак, оскільки RC4 залишається уразливим шифром, то відповідно і TKIP вважається уразливим.

3) Протокол WPA2. Цей протокол є згаданим раніше стандартом IEEE 802.11i. У якості основного шифру був обраний стійкий блоковий шифр AES. Система автентифікації, у порівнянні з WPA, зазнала мінімальних змін. Як і у його попередники, автентифікація може реалізуватись двома методами (WPA2-Enterprise та WPA2-PSK). Для криптографічної оброблення використовується стандарт AES-CCMP, тобто для шифрування – AES, а розподіл ключів та перевірка цілісності виконана у одному компоненті CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol). Варто також зазначити, що деякі виробники під WPA з AES-CCMP мають на увазі WPA2 з AES-CCMP. Таким чином, щоб не плутатись, під WPA будемо мати на увазі WPA-TKIP (тобто автентифікацію WPA з методом шифрування TKIP), а під WPA2 – WPA2 з AES-CCMP (тобто автентифікацію WPA2 з методом шифрування AES–CCMP).

Методи обмеження доступу до бездротових мереж

Взагалі, методів обмеження доступу по суті є два – це відключення широкомовного розсилання ESSID (ідентифікатор точки доступу, а фактично – ім'я бездротової мережі) та фільтрація MAC-адрес.

1) У першому випадку Access Point (AP) не передає у відкриту свій ESSID. Для підключення до такої мережі потрібно знати її ESSID, у іншому випадку підключення неможливе.

2) У другому випадку можливі такі три варіанти конфігурації:

а) AP приймає з'єднання з всіма бездротовими пристроями, незалежно від їх MAC-адреси;

б) AP не приймає з'єднання з бездротовими пристроями, MAC-адреси яких задані у списку безпосередньо на самому пристрої. Усі інші пристрої можуть підключатися;

в) AP приймає з'єднання лише з тими пристроями, MAC-адреси яких задані у списку безпосередньо на самому пристрої. Усі інші пристрої не можуть підключатися.

З точки зору безпеки рекомендується завжди використовувати останній режим!

Методи автентифікації у бездротових мережах:

1) Open System Authentication. У даному випадку клієнт відсилає точці доступу запит з її ідентифікатором (MAC-адресою). AP перевіряє, чи проходить клієнт за списком MAC-адрес (якщо він включений), потім перевіряється відповідність WEP-ключів (якщо включено WEP-шифрування). Підтримується роумінг між точками доступу. Можливі режими шифрування: без шифрування, статичний WEP, CKIP (Cisco Key Integrity Protocol, рання версія протоколу TKIP).

2) Open System Authentication with EAP. Попередній варіант автентифікації може використовуватися спільно з автентифікацією через протоколи EAP на RADIUS сервері. Можливі режими шифрування: без шифрування, динамічний WEP, CKIP.

3) Shared System Authentication. У цьому випадку клієнт відсилає запит на з'єднання з точкою доступу. Потім AP відсилає клієнтові послідовність, яку він шифрує і відсилає назад. Якщо послідовність зашифрована вірно, то автентифікація проходить успішно. Варто відмітити, що у даному варіанті захист слабкіший, ніж у випадку Open System. Можливі режими шифрування: без шифрування, динамічний WEP, CKIP.

Види атак на Wi-Fi мережу:

– *Access Point Spoofing & Mac Sniffing.* Список доступу цілком придатний до використання спільно з правильною ідентифікацією користувачів у цьому списку. У випадку ж із MAC-адресою Access Control List дуже просто подолати, оскільки таку адресу дуже просто змінити (бездротові мережеві карти дозволяють програмно міняти MAC-адресу) і ще простіше перехопити, оскільки він навіть у випадку з WEP передається у відкритому вигляді. Таким чином, елементарно проникнути у мережу, захищену Access Control List і використовувати усі її переваги та ресурси. У разі наявності у порушника власної точки доступу є інша можливість: встановлюється AP поряд з існуючою мережею – якщо сигнал

хакера сильніший оригінального, то клієнт підключиться саме до хакера, а не до мережі, передавши при цьому не тільки MAC-адресу, але пароль та інші дані.

– *WEP Attacks.* Для розуміння даних атак необхідно розглянути детально протокол WEP (рис. 2.1.2). Спочатку чисті дані проходять перевірку цілісності і видається ICV. У протоколі 802.11 для цього використовується CRC-32. ICV додається в кінець даних. Генерується 24-бітний IV і до нього «прив'язується» секретний ключ. Набуте значення є початковим для генерації ПВП. Генератор видає ключову послідовність. Вектор ініціалізації додається у кінець і все це передається в ефір.

– *Plaintext атака.* Під час реалізації такої атаки зловмисник знає початкове послання і має копію зашифрованої відповіді. Ланка, якої не вистачає і є ключем. Для його отримання зловмисник посилає до цілі невелику частину даних і одержує відповідь. Одержавши його, хакер знаходить 24-бітний IV, використовуваний для генерації ключа: знаходження ключа у такому разі – це лиш не складна задача спеціалізованого ПЗ. Інший варіант – звичайний XOR. Якщо у хакера є відправлений plain text і його зашифрований варіант, то він просто підбирає шифр і на виході одержує ключ, який разом з вектором дає можливість «завантажити» пакети у мережу без автентифікації на точці доступу.

– *Повторне використання шифру.* Зловмисник відбирає з пакету ключову послідовність. Оскільки алгоритм шифрування WEP на вектор відводить досить мало місця, атакуючий може перехопити ключовий потік, використовуючи різні IV, створюючи для себе їх послідовність. Таким чином, зловмисник може розшифрувати повідомлення, використовуючи все той же XOR, коли мережею підуть зашифровані дані.

– *Атака Fluther-Mantin-Shamir (FMS атака).* Ця атака є першою запропонованої атакою (у 2001 р.) на мережі з WEP-шифрування даних. Вимагає, щоб пакети містили «слабкі» (уразливі) IV (Weak IV). Необхідна кількість перехоплених пакетів – від півмільйона і вище. Зберігати можна тільки самі IV. При відсутності «слабких» IV (наприклад, після корекції алгоритму шифрування, внаслідок «роботи над помилками» розробника у новій прошивці) атака є неефективною.

– *Low-Hanging Fruit.* Цей вид атаки розрахований на здобування незахищених ресурсів з незахищених мереж. Більшість бездротових мереж є абсолютно незахищеними, у них не вимагається авторизація і навіть не використовується шифрування WEP. Таким чином, людина з бездротовою мережевою карткою і сканером може легко підключитися до AP і використати усі необхідні ресурси. Звідси і назва – «фрукти, що низько висять, зірвати які не складає жодних труднощів».

– *Атака KoreK ChopChop.* Кількість необхідних унікальних IV – кілька сотень тисяч, для ключа довжиною 128 біт. Головна вимога – щоб IV не збігалися між собою. Абсолютно не важливо наявність слабких IV. Зберігати можна тільки IV. Ця атака дозволяє розшифрувати окремий пакет, не знаючи ключа WEP. Атака була запропонована у 2004 р. Принцип дії: повторно відсилається зашифрований пакет, попередньо модифікуючи один

байт. Потім дивимося на реакцію AP, далі визначається вихідне значення байта і переходимо до наступного. Таким чином, постійно посилаючи пакети, можливо розшифрувати трафік, навіть якщо кожен клієнт використовує свій унікальний ключ.

– *PTW атака.* Така атака дозволяє прискорити процес знаходження WEP-ключа, коли перехоплюється велика кількість ARP-пакетів. Атака з'явилася внаслідок появи методу інжекція ARP-запитів у бездротову мережу. Не використовувати подібну можливість було б нерозумно. Для крипто аналізу потрібно зберігати вміст усього перехопленого пакета даних. Кількість необхідних пакетів – кілька десятків тисяч. На сьогодні – це найбільш ефективна атака. Єдиний мінус – майже завжди потрібно проводити активну атаку на бездротову мережу, так як ARP-запити при нормальному функціонуванні мережі фактично відсутні.

– *DoS-атаки на бездротову мережу.* Існують три варіанти таких атак: 1) на фізичному рівні моделі OSI (необхідне спеціальне обладнання, наприклад, заглушка); 2) на канальному рівні і вище (необхідно звичайний бездротовий адаптер); 3) використовують особливості конкретного обладнання. У першому випадку глушиться діапазон Wi-Fi (2,4 Ггц), крім Wi-Fi мереж ще глушаться усі Bluetooth-пристрої у радіусі дії. У другому випадку, в залежності від типу шифрування і автентифікації, проводитимуться спеціальні дії: деавтентіфікація клієнтів або посилка від їх MAC помилкових пакетів. У третьому випадку використовуються апаратні і програмні уразливості бездротових клієнтів і точки доступу.

Основні способи захисту бездротових мереж:

1) Фільтрація MAC-адрес. У цьому випадку адміністратор складає список MAC-адрес мережевих карт клієнтів. У разі декількох AP необхідно передбачити, щоб MAC-адреса клієнта існувала на усіх, щоб він міг безперешкодно переміщатися між ними. Проте, цей метод захисту дуже легко подолати, так що поодинці його використовувати не рекомендується.

2) ESSID – використання системи мережевих ідентифікаторів. При спробі клієнта підключитися до AP на нього передається семизначний алфавітно-цифровий код. Використовуючи мітку SSID, можна бути упевненим, що до мережі зможуть під'єднатися тільки клієнти, що знають його.

3) Firewall. Доступ до мережі повинен здійснюватися за допомогою IPSec, Secure Shell або VPN, брандмауер повинен бути налаштований на роботу саме з цими мережевими з'єднаннями.

4) AP треба налаштувати на фільтрацію MAC-адрес, крім того, фізично сам пристрій необхідно ізолювати від оточуючих. Рекомендується також конфігурувати точку тільки за telnet (мережевий протокол для реалізації текстового інтерфейсу у мережі), відключивши можливість конфігурації через браузер або SNMP.

Практичні рекомендації щодо налаштування безпечної домашньої бездротової мережі:

1) Домашня локальна мережа повинна функціонувати у режимі WPA2-PSK із шифруванням AES-CCMP (відповідно до сучасного рівня обчислювальних засобів зламування не є можливим) і включеним фільтром MAC-адрес, у якому мають бути перераховані усі без виключення MAC-адреси бездротових адаптерів комп'ютерів, які мають право підключатися до цієї мережі.

2) Ключ для доступу (PreSharedKey – PSK) не повинен бути словом або кількома словами. Він повинен бути послідовністю літер та цифр.

3) ESSID точки доступу може бути яким завгодно (на розсуд користувача), тільки не значенням за замовчуванням.

Дотримання цих основних правил дасть повну гарантію, що ніхто інший не зможе підключитися до домашньої бездротової мережі, за умови, що ключ доступу зберігається у секреті. Підводячи підсумки, варто зазначити, що на сьогоднішній день безпеці конфіденційної інформації у бездротових мережах необхідно надавати особливу увагу. Адже бездротова мережа має великий радіус дії, і тому зловмисник може перехоплювати інформацію або ж атакувати мережу, знаходячись на безпечній відстані. У наш час існує безліч різних способів захисту і, за умови правильного налаштування, можна бути упевненим в забезпеченні необхідного рівня безпеки.

Контрольні запитання

1) Що таке Wi-Fi?

2) Які стандарти входять до серії IEEE 802.11?

3) Які є методи шифрування у бездротових мережах? Котрі з них рекомендовано використовувати і чому?

4) Який метод автентифікації у бездротових мережах є найефективнішим? За рахунок чого?

5) Які є методи обмеження доступу у бездротових мережах?

6) Які є сучасні атаки на Wi-Fi мережі?

7) Які існують основні заходи щодо захисту бездротових мереж?

8) Що таке вектор ініціалізації (IV) і яка його роль в управлінні ключовими даними за протоколом WEP?

9) Порівняйте WPA та WPA2 з точки зору інформаційної безпеки і застосовуваних протоколів автентифікації, шифрування, забезпечення цілісності і т.п.

10) Сформулюйте практичні рекомендації щодо налаштування безпечної домашньої бездротової мережі.

Тема 8. Особливості побудови систем автентифікації

Поняття автентифікації та її основні методи. *Автентифікація (Authentication)* – процедура перевірки приналежності користувачеві чи процесу користувача права доступу на підставі пред'явленого ним ідентифікатора. Цей процес може бути оберненим, тобто, коли перевірку здійснює користувач чи процес користувача, наприклад, з метою впевнитися, що в ідентифіковану систему можна безпечно вводити конфіденційну інформацію. Як синонім цього поняття інколи використовують такі словосполучення: «перевірка достовірності», «пред'явлення повноважень» тощо.

Автентифікацію не слід плутати з ідентифікацією та авторизацією. *Ідентифікація (Identification)* – це присвоєння особі ідентифікатора (ознака, яка служить для ідентифікації особи чи предмета, що розпізнається) або порівняння ідентифікатора з переліком привласнених ідентифікаторів (наприклад, ідентифікація за штрих-кодом), *автентифікація (Authorization)* – це встановлення відповідності особи представленому нею ідентифікатору, а *авторизація,* в свою чергу, – це надання цій особі можливостей відповідних наданим їй правам або перевірка наявності прав при виконані будь-яких дій.

Автентифікація буває *односторонньою* (зазвичай клієнт доводить свою справжність серверу) і *двосторонньою (взаємною).* Прикладом односторонньої автентифікації є процедура входу користувача у систему. Одним із способів автентифікації в комп'ютерній системі є введення ідентифікатора, так званого *логіна (Login)* і *пароля (Password)* – деякої конфіденційної інформації, знання якої забезпечує володіння певним ресурсом. Отримавши введені користувачем логін і пароль, комп'ютер порівнює їх із значенням, яке зберігається в спеціальній базі даних і, в разі збігу, пропускає користувача в систему.

На комп'ютерах з ОС сімейства Unix базою є файл */etc/master.passwd* (у дистрибутивах Linux зазвичай файл /etc/shadow, доступний для читання лише root), в якому паролі користувачів зберігаються у вигляді геш-функцій від відкритих паролів, крім того, у цьому ж файлі зберігається інформація про права користувача. Спочатку, в Unix-системах пароль (в зашифрованому вигляді) зберігався у файлі /etc/passwd, доступному для читання всім користувачам, що було небезпечно. На комп'ютерах з ОС Windows NT/2000/XP/2003 така БД називається SAM (Security Account Manager – диспетчер захисту облікових записів). База SAM зберігає облікові записи користувачів, що включають в себе всі дані, необхідні системі захисту для функціонування. Знаходиться вона у директорії *%windir%\system32\config*. У доменах Windows Server 2000/2003 такою базою є Active Directory.

Однак більш надійним способом зберігання автентифікаційних даних визнано використання спеціальних апаратних засобів (компонентів). При необхідності забезпечення роботи співробітників на різних комп'ютерах (з підтримкою системи безпеки) використовують апаратно-програмні системи, що дозволяють зберігати автентифікаційні

дані і криптографічні ключі на сервері організації. Користувачі можуть вільно працювати на будь-якому комп'ютері, маючи доступ до своїх автентифікаційних даних і криптографічних ключів.

Процедура автентифікації використовується при обміні інформацією між комп'ютерами, при цьому використовуються дуже складні криптографічні протоколи, що забезпечують захист лінії зв'язку від прослуховування або підміни одного з учасників взаємодії. А оскільки, як правило, автентифікація необхідна обом об'єктам, що встановлюють мережеве з'єднання, то автентифікація повинна бути взаємною.

Зокрема, в ОС сімейства Windows NT 4 використовується протокол NTLM (NT LAN Manager – диспетчер локальної мережі NT). А у доменах Windows 2000/2003 застосовується набагато більш досконалий протокол Kerberos.

Прийнято виділяти два основних класи автентифікації: одночинникова та багаточинникова. Розглянемо основні методи *одночинникової автентифікації* у комп'ютерних системах за принципом наростаючої складності.

Базова автентифікація. При використанні такого виду автентифікації ім'я користувача та пароль включаються до складу web-запиту (HTTP POST або HTTP GET). Зловмисник, що перехопив пакет, легко отримує секретну інформацію. Навіть якщо контент з обмеженим доступом не надто важливий, цей метод краще не використовувати, тому що користувач може застосовувати один і той же пароль на декількох web-сайтах. Опитування Sophos показують, що 41% у 2006 р. і 33% в 2009 р. користувачів застосовують для всієї своєї діяльності в Інтернет всього один пароль, чи то сайт банку, чи розважальний форум. Також, серед недоліків парольної автентифікації слід зазначити невисокий рівень безпеки – пароль можна підглянути, вгадати, підібрати тощо.

Дайджест-автентифікація. При даній автентифікації пароль користувача передається в гешованому вигляді. Здавалося б, що за рівнем конфіденційності паролів цей тип мало чим відрізняється від попереднього, так як атакуючому все одно, чи дійсно це справжній пароль, чи тільки геш від нього: перехопивши повідомлення, він все одно отримує доступ до кінцевої точки. Але це не зовсім так – пароль гешується завжди з додаванням довільного рядка символів, що генерується на кожне з'єднання заново. Таким чином, при кожному з'єднанні генерується новий геш паролю і перехоплення його нічого не дасть. Дайджест-автентифікація підтримується всіма популярними серверами і браузерами.

HTTPS. Протокол HTTPS дозволяє шифрувати усі дані, передані між браузером і сервером, а не тільки імена користувачів і паролі. Протокол HTTPS (заснований на системі безпеки SSL) слід використовувати у випадку, якщо користувачі повинні вводити важливі особисті дані – адреса, номер кредитної карти або банківські відомості. Проте, використання HTTPS значно уповільнює швидкість доступу.

Механізми автентифікації із застосуванням *цифрових сертифікатів,* як правило, використовують протокол із запитом і відповіддю. Сервер автентифікації відправляє

користувачу послідовність символів, так званий запит. Як відповідь виступає запит сервера автентифікації, підписаний за допомогою закритого ключа користувача. Автентифікація з відкритим ключем використовується як захищений механізм автентифікації в таких протоколах як SSL, а також може використовуватися як один з методів автентифікації в рамках протоколів Kerberos і RADIUS.

Cookies. Безліч різних сайтів використовують як засіб автентифікації cookies, до них відносяться: чати, форуми, ігри. Якщо cookies вдасться викрасти, то, підробивши його, можна автентифікуватися у якості іншого користувача. У випадку, коли дані, що вводяться, погано фільтруються або не фільтруються зовсім, викрасти cookies стає не дуже складним завданням. Щоб якось поліпшити ситуацію використовується захист за IP-адресою, тобто cookies сесії зв'язуються з IP-адресою, з якого спочатку користувач авторизувався в системі. Однак, IP-адресу можна підробити використовуючи IP-спуфінг (IP-spoofing), тому сподіватися на захист за IP-адресою теж не можна. Сьогодні більшість браузерів використовують cookie з позначкою «HTTPonly», який забороняє доступ до cookies різних скриптів.

Децентралізована автентифікація (OpenID, OpenAuth, OAuth). Одним з головних мінусів таких систем є те, що злом дає доступ відразу до багатьох сервісів. OpenID – децентралізована система автентифікації користувачів. OpenID дозволяє користувачеві мати один логін / пароль для різних web-сайтів. Безпека забезпечується підписуванням повідомлень. Передача ключа для цифрового підпису заснована на використанні алгоритму Діффі-Хеллмана, також можлива передача даних за HTTPS. Можливі уразливості OpenID:

- фішинг (Phishing);
- атака людина посередині (man-in-the-middle attack, MitM).

Автентифікація за OpenID зараз активно використовується і надається такими гігантами, як BBC, Google, IBM, Microsoft, MySpace, PayPal, VeriSign, Yandex і Yahoo!

OpenAuth використовується для автентифікації AOL (американська медіа компанія, власник четвертої за популярністю пошукової системи у світі) користувачів на web-сайтах. Дозволяє їм користуватися сервісами AOL, а також будь-якими іншими надбудованими над ними, крім того, дозволяє проходити автентифікацію на сайтах, що не відносяться до AOL, при цьому не створюючи нового користувача на кожному сайті. Протокол функціонує схожим на OpenID чином. Також, прийняті додаткові заходи безпеки:

- дані сесії (у т.ч. інформація про користувача) зберігаються не у cookies;
- cookies автентифікації шифруються за алгоритмом «PBEWithSHAAnd3-KeyTripleDES-CBC»;
- доступ до cookies автентифікації обмежений певним доменом так, що інші сайти не мають до них доступу (у тому числі сайти AOL).

OAuth дає можливість користувачеві дозволити одному Інтернет-сервісу отримати доступ до даних користувача на іншому Інтернет-сервісі. Протокол використовується у

таких системах як Twitter, Google (Google також підтримує гібридний протокол, який об'єднує в собі OpenID та OAuth).

Відстеження автентифікації самим користувачем. Багато у чому безпека користувачів в Інтернет залежить від поведінки самих користувачів. Так, наприклад, Google показує з якої IP-адреси включені користувацькі сесії, логує авторизацію, дозволяє здійснити такі налаштування:

– передача даних тільки за HTTPS;

– Google може детектувати, що зловмисник використовує Ваш аккаунт (друзі вважають Ваші листи спамом, остання активність відбувалася в нехарактерний для Вас час, деякі повідомлення зникли тощо);

– відстеження списку третіх сторін, що мають доступ до використовуваних користувачем продуктів Google.

Найчастіше користувачеві повідомляється з якої IP-адреси він останній раз проходив автентифікацію.

Багаточинникова автентифікація. Для підвищення безпеки на практиці використовують кілька чинників автентифікації відразу. У процесі багаточинникової автентифікації використовуються чинники різної природи:

– властивість, якою володіє суб'єкт (інколи називають «те, що Ви собою являєте»). Наприклад, біометрія, природні унікальні відмінності: обличчя, відбитки пальців, райдужна оболонка очей, капілярні узори, послідовність ДНК тощо;

– знання – інформація, яку знає суб'єкт («те, що Ви знаєте»). Наприклад, пароль, пін-код тощо;

– володіння – річ, яку має суб'єкт («те, що Ви маєте»). Наприклад, електронна або магнітна карта, електронний ключ, флеш-пам'ять.

В основі одного з найнадійніших на сьогоднішній день методів багато-чинникової автентифікації лежить застосування персональних апаратних пристроїв – токенів. По суті, токен – це смарт-карта або USB-ключ. Токени дозволяють генерувати і зберігати ключі шифрування, забезпечуючи тим самим сувору автентифікацію. Використання класичних «багаторазових» паролів є серйозною уразливістю при роботі з чужих комп'ютерів, наприклад в Інтернет-кафе. Це підштовхнуло провідних виробників ринку автентифікації до створення апаратних генераторів одноразових паролів. Такі пристрої генерують черговий пароль або за розкладом (наприклад, кожні 30 секунд), або за запитом (при натисканні на кнопку). Кожен такий пароль можна використовувати тільки один раз. Перевірку правильності введеного значення на стороні сервера перевіряє спеціальний сервер автентифікації, який обчислює поточне значення одноразового пароля програмно. Для збереження принципу двочинникової автентифікації крім згенерованого пристроєм значення користувач вводить постійний пароль.

Ідентифікація/автентифікація за допомогою біометричних даних

Біометрія являє собою сукупність автоматизованих методів ідентифікації та автентифікації людей на основі їх фізіологічних і поведінкових характеристик. До числа фізіологічних характеристик належать особливості відбитків пальців, сітківки та рогівки очей, геометрія руки й обличчя і т.п. До поведінкових характеристик відносяться динаміка підпису, стиль роботи з клавіатурою тощо.

У загальному вигляді робота з біометричними даними організована таким чином. Спочатку створюється БД характеристик потенційних користувачів. Для цього біометричні характеристики користувача знімаються, обробляються і результат оброблення (біометричний шаблон) заноситься в базу даних.

Надалі для ідентифікації (і одночасно автентифікації) користувача процес зняття та оброблення повторюється, після чого проводиться пошук у базі даних шаблонів. У разі успішного пошуку особу користувача та її справжність вважають встановленими. Для автентифікації досить провести порівняння з одним біометричних шаблоном, обраним на основі попередньо введених даних. У табл. 3 наведено порівняльний аналіз властивостей біометричних характеристик людини.

Таблиця 3.

Експертна оцінка властивостей біометричних характеристик людини:

(+ + + – висока оцінка, + + – середня, + – низька)

Характеристика	Універсальність	Унікальність	Сталість	Вимірюваність
Відеообраз обличчя	+++	+	++	+++
Термограмма обличчя	+++	+++	+	+++
Відбиток пальця	++	+++	+++	++
Геометрія руки	++	++	++	+++
Райдужна оболонка ока	+++	+++	+++	++
Сітківка	+++	+++	++	+
Підпис	+	+	+	+++
Голос	++	+	+	++
Відбиток губ	+++	+++	++	+
Особливості вуха	++	++	++	++
Динаміка підпису	+++	+++	+	+++
Хода	+++	++	+	+

Зазвичай біометрію застосовують разом з іншими автентифікаторами, такими, наприклад, як інтелектуальні карти. Іноді біометрична автентифікація є лише першим рубіжом захисту і служить для активізації інтелектуальних карт, що зберігають криптографічні секрети; у такому випадку біометричний шаблон зберігається на тій же картці. Необхідно враховувати, що біометрія уразлива до тих же загроз, що й інші методи

автентифікації. По-перше, біометричний шаблон порівнюється не з результатом первісної оброблення характеристик користувача, а з наявним на цей час. По-друге, біометричні методи не більш надійні, ніж БД шаблонів. По-третє, слід враховувати різницю між застосуванням біометрії на контрольованій території, під пильним оком охорони, і в «польових» умовах, коли, наприклад, до пристрою сканування рогівки можуть піднести муляж і т.п. По-четверте, біометричні дані людини змінюються, так що база шаблонів потребує контролю за змінами, що створює певні проблеми і для користувачів, і для адміністраторів.

Але головна небезпека полягає в тому, що будь-яка «пробоїна» для біометрії виявляється фатальною. Паролі, при всій їх ненадійності, у крайньому випадку можна змінити. Втрачену автентифікаційну карту можна анулювати і завести нову. Палець, очі або голос змінити не можна. Якщо біометричні дані виявляться скомпрометовані, доведеться, як мінімум, виробляти істотну модернізацію всієї системи.

Парольні системи, паролі та вимоги до управління ними

Під парольного системою розуміється програмно-апаратний комплекс, який реалізує системи ідентифікації та автентифікації користувачів автоматизованої системи на основі одноразових і багаторазових паролів. Як правило, такий комплекс функціонує спільно з підсистемами розмежування доступу і реєстрації подій. У окремих випадках парольна система може виконувати ряд додаткових функцій, зокрема, генерацію та розподіл короткочасних (сеансових) криптографічних ключів.

Парольна система являє собою «передній край оборони» всієї системи безпеки. Деякі її елементи (зокрема, інтерфейс користувача) можуть бути розташовані у місцях, відкритих для доступу потенційному зловмиснику. Тому, парольна система стає одним з перших об’єктів атаки при вторгненні зловмисника у захищену систему.

До типів загроз безпеки парольних систем відносяться: 1) Розголошення параметрів облікового запису; 2) Втручання у функціонування компонентів парольної системи.

Існують такі найбільш поширені методи отримання паролів:

– *метод тотального перебору:* перевірка всіх ключів послідовно;

– *словникова атака* – для перебору використовується словник найбільш ймовірних ключів. У словник зазвичай входять: a) відома особиста інформація про власника пароля; b) словникова БД, складена з імен людей, героїв мультфільмів і міфічних тварин, лайки, чисел, назв фільмів тощо; c) слова, що отримані внесенням різних змін у словникову базу даних (наприклад, зміна регістру символів, транслітерація, зміна порядку написання слова, заміна літер «о» на цифру «0», «і» – на «1» тощо); d) пари слів;

– *перевірка паролів,* які встановлюються у системах за замовчуванням (різновид словникової атаки). У деяких випадках адміністратор ПЗ, встановивши або отримавши новий продукт від розробника, не спромагається перевірити, з чого складається система безпеки.

Як наслідок, пароль, встановлений фірмою-розробником за замовчуванням, залишається основним паролем в системі;

– *отримання паролів із самої системи* на основі програмної і апаратної реалізації конкретної системи. Основними двома можливостями з'ясування пароля є: НСД до носія, який містить паролі, або використання уразливостей: помилок і недокументованих можливостей у реалізації системи;

– *атаки на основі соціальної психології (соціальний інжиніринг)* – можуть приймати самі різні форми. Наприклад, зі списку співробітників вибирається той, хто не використовував пароль протягом декількох днів (відпустка, відгули, відрядження) і кого адміністратор не знає за голосом. Потім слідує дзвінок адміністраторові з поясненням ситуації про забутий пароль, щирі вибачення, прохання зачитати пароль або змінити його на новий. Можлива і зворотна схема – звернення до співробітника нібито від служби безпеки.

Можливі такі *варіанти зберігання паролів* в базі даних облікових записів (відразу зауважимо, що найбільший інтерес викликають другий і третій способи):

1) у відкритому вигляді; 2) у вигляді згорток (геш-значень); 3) зашифрованими на деякому секретному ключі.

Гешування не забезпечує захист від підбору паролів за словником у разі отримання бази даних зловмисником. При виборі алгоритму гешування, який буде використаний для обчислення геш-функції паролів, необхідно гарантувати розбіжність їх значень, отриманих на основі різних паролів користувачів. Крім того, слід передбачити механізм, що забезпечує унікальність гешів у тому випадку, якщо два користувача вибирають однакові паролі. При цьому, при обчисленні кожної геш-функції зазвичай використовують деяку кількість «випадкової» інформації, наприклад, що видається ГПВП.

При шифруванні паролів особливе значення має *спосіб генерації і зберігання ключа шифрування* бази даних облікових записів. Деякі можливі варіанти:

1) генерується програмно і зберігається в системі, забезпечуючи можливість її автоматичного перезавантаження;

2) генерується програмно і зберігається на зовнішньому носії, з якого зчитується при кожному запуску;

3) генерується на основі обраного адміністратором пароля, який вводиться в систему при кожному запуску.

У другому випадку необхідно забезпечити неможливість автоматичного перезапуску системи, навіть якщо вона виявляє носій з ключем. Для цього можна вимагати від адміністратора підтвердження продовження процедури завантаження. Найбільш безпечне зберігання паролів забезпечується при їх гешуванні і подальшому шифруванні отриманих гешів, тобто при комбінації другого і третього способів.

Контрольні запитання

1) Що таке «автентифікація»? У чому її відмінність від таких суміжних понять, як «ідентифікація» та «авторизація»?

2) Особливості зберігання бази даних автентифікації на комп'ютерах з ОС сімейства Unix та Windows?

3) Які є методи одночинникової автентифікації в ІКС та у чому вони полягають?

4) Що таке багаточинникова автентифікація? Які основні чинники використовуються у процесі її проведення?

5) У чому полягає автентифікація за допомогою біометричних даних? Використання яких біометричних ознак на сьогодні є найбільш ефективним?

6) Які існують методи отримання паролів? У чому вони полягають?

7) Які є основні способи зберігання паролів?

8) Які є способи генерації і зберігання ключів шифрування бази даних облікових записів?

9) Чому біометричну автентифікацію зазвичай використовують поряд з іншими автентифікаторами?

10) Охарактеризуйте популярні на сьогодні системи децентралізованої автентифікації.

Тема 9. Принципи побудови ІКС на базі квантових технологій. Квантовий розподіл ключів та прямий безпечний зв'язок

Основи квантової криптографії. В останні роки значний інтерес серед світової наукової спільноти викликають системи захисту інформації на базі методів квантової криптографії. *Квантова криптографія* – це наука, що вивчає методи захисту систем зв'язку і базується на принциповій непорушності постулатів квантової фізики (механіки), об'єкти якої (фотони, фонони, гравітони) забезпечують процеси безпечної передачі інформації між легітимними користувачами.

Зазначеними *постулатами квантової механіки* є *постулат вимірювання* (наслідок із принципу невизначеності Гейзенберга) та так звана *теорема про заборону клонування.* Згаданий ***принцип невизначеності*** **–** це фундаментальна нерівність (відношення невизначеностей), згідно якої усі динамічні параметри діляться на дві взаємодоповнюючі групи (перша – часові та просторові координати; друга – імпульс та енергія), при чому неможливо одночасно виміряти параметри з різних груп, наприклад, місцеположення та енергію об'єкта.

Теорема про заборону клонування стверджує неможливість створення точних (на 100 %) копій квантових об'єктів на відміну від класичних. Ці властивості, не притаманні класичним системам зв'язку, і забезпечують *теоретико-інформаційну (абсолютну, безумовну) стійкість* квантової криптографії.

Вагоме місце у квантовій криптографії займає квантовий розподіл ключів (КРК), проте також варто виділи такі напрями як: квантовий прямий безпечний зв'язок (КПБЗ), квантове розділення секрету (КРС), квантовий потоковий шифр (КПШ), квантовий цифровий підпис (КЦП) та квантова стеганографія (рис. 30).

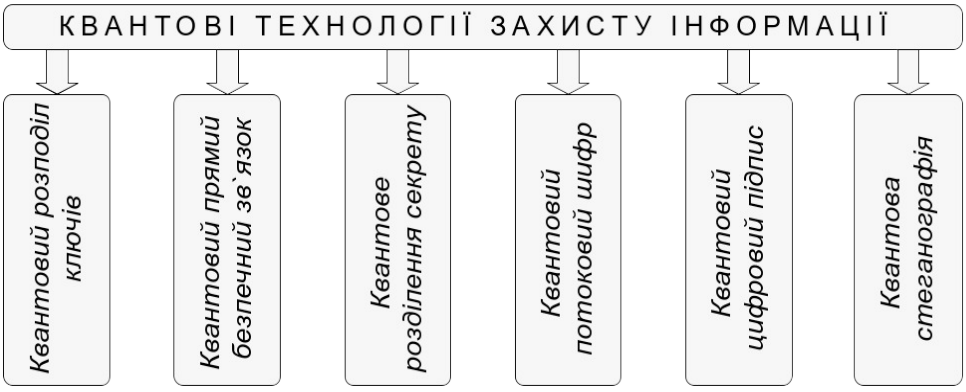

Рис. 30. Квантові технології захисту інформації

На рис. 31 зображено узагальнену класифікацію методів квантової криптографії за такими базовими ознаками, як *призначення методів квантової криптографії (у певних задачах захисту інформації)* та *використовувані квантові технології:*

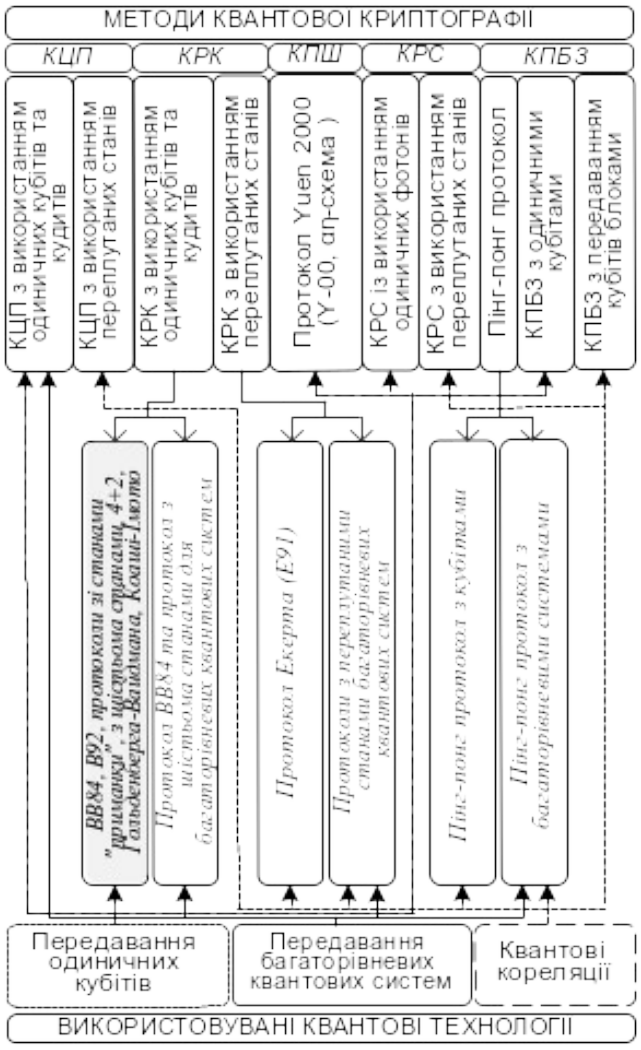

Рис. 31. Узагальнена класифікація методів квантової криптографії

1) Першою ознакою є *призначення методів квантової криптографії.* Більшість таких методів є, в деякій мірі, аналогами існуючих класичних (традиційних) методів і виконують відповідні їм функції. Як уже зазначалось, *квантові методи* поділяються на: розподіл ключів, прямий безпечний зв'язок, розділення секрету, потоковий шифр, цифровий підпис та стеганографію. Як згадувалося раніше, *майже усі квантові методи мають відповідні класичні аналоги: КРК* вирішує важливу проблему класичної криптографії з секретним ключем і його функціональними аналогами у класичній криптографії є такі методи розподілу ключів: теоретико-інформаційна схема, криптографічна схема з відкритим ключем, симетрична криптографічна схема з обчислювальною стійкістю і навіть схема застосування довіреного кур'єра. *КПБЗ* – єдина квантова технологія, що не має аналогів у класичному захисті інформації (якщо не рахувати схему застосування відвідного каналу), так як теоретико-інформаційна стійкість цього методу забезпечується за відсутності криптографічної оброблення інформації (у принципі, КПБЗ може також використовуватись і для розподілу ключів шифрування, тоді аналогами будуть зазначені класичні схеми розподілу ключів). Відповідно, *КПШ* є аналогом класичного потокового шифру, КРС –

класичної системи розділення секрету, метою КЦП, як і класичного ЕЦП, є підтвердження цілісності переданих документів та ідентифікація підписувача (відправника, автора). Квантова стеганографія є найменш досліджуваною технологією захисту інформації на основі квантових технологій і полягає у прихованні самого факту передачі інформації (як і в класичному аналозі) за допомогою квантових кореляцій (властивостей квантових переплутаних станів), проте на сьогодні вчені знаходять у пошуку оптимального алгоритму приховування одного квантового стану в іншому.

2) Другою базовою ознакою для класифікації методів квантової криптографії є *використовувані квантові технології.* За цією ознакою варто виділити три основні напрямки квантових технологій:

- передавання одиничних кубітів;
- передавання багаторівневих квантових систем (кудитів);
- використання квантових переплутаних станів (квантові кореляції).

Перший напрямок – **передавання одиничних квантових систем (кубітів)** – заснований на кодуванні квантового стану кубітів і базується на принципі неможливості абсолютно надійно розрізнити два неортогональні квантові стани. Захищеність цієї технології ґрунтується на теоремі про заборону клонування невідомого квантово стану – завдяки унітарності та лінійності квантової механіки, неможливо створити точну копію невідомого квантового стану з боку зловмисника – це унеможливлює створення точних копій станів фотонів за умов використання будь-якого обладнання. Відповідно рис. 2.4.2 основними протоколами, що використовують цю технологію, є протоколи КРК *BB84, B92, протоколи зі станами «приманки», протокол з шістьома станами, протокол 4+2, протокол Гольденберга-Вайдмана, протокол Коаші-Імото*, протоколи КПБЗ *з одиничними кубітами,* протоколи КРС *з використанням одиничних поляризованих фотонів,* протокол КПШ *Yuen 2000,* протоколи КЦП *на основі одиничних кубітів.*

Другий перспективний напрямок квантових технологій – це **передавання багаторівневих квантових систем (кудитів).** Останнім часом, значно зріс інтерес до використання багаторівневих кудитів, так як існує небезпідставне припущення, що квантові системи на їх основі більш ефективно розв'язують деякі задачі, наприклад, у квантових системах узагальнення на багаторівневі системи значно підвищує інформаційну місткість носіїв – це збільшує можливу кількість інформації, яка може бути переданою за один цикл протоколу. До таких протоколів відносять: протоколи КРК *BB84 та з шістьома станами для багаторівневих квантових систем,* а також протокол КРК *з переплутаними станами багаторівневих квантових систем,* у КПБЗ *пінг-понг протокол з багаторівневими квантовими системами* та протокол КЦП *з використанням кудитів.*

І нарешті, третя технологія – це **використання властивостей квантових переплутаних станів (квантових кореляцій)**. Дві квантово-механічні системи можуть знаходитися у стані взаємної кореляції таким чином, що вимірювання певного параметру в

одній системі визначить результат вимірювання даного параметру у іншій системі. Математично, квантова кореляція представляє собою нефакторизуємий багаточастинковий квантовий стан (тобто стан, що не можливо розкласти на множники – представити у вигляді добутку кількох станів) – це означає, що об'єкти, з яких складається квантова переплутана система, не мають власних хвильових функцій і векторів квантових станів – їх стани є переплутаними і описати їх можна лиш за допомогою матриці густини (один із способів опису квантово-механічної системи, який, на відміну від хвильової функції, може задавати чисті та переплутані квантові стани). Базовими протоколами, основаними на квантових кореляціях, є протоколи КРК *Екерта та з переплутаними станами багаторівневих квантових систем,* протокол КЦП *з використанням переплутаних станів,* у КПБЗ *пінг-понг протокол з кубітами та багаторівневими квантовими системами, протоколи з передаванням кубітів блоками,* а також протоколи КРС *з використанням переплутаних станів.*

Квантовий розподіл ключів

Ідея використання квантових об'єктів для захисту інформації була вперше запропонована у 1970 р. С. Вейснером. У 1984 році Ч. Беннет з компанії IBM та Ж. Брассар з Монреальського університету розвинули ідею Вейснера і запропонували *перший протокол квантової криптографії BB84* (установка якого наведена на рис. 32), що мав стати альтернативним і нетрадиційним вирішенням проблеми розподілу ключів шифрування (актуальної для криптографії уже на той час).

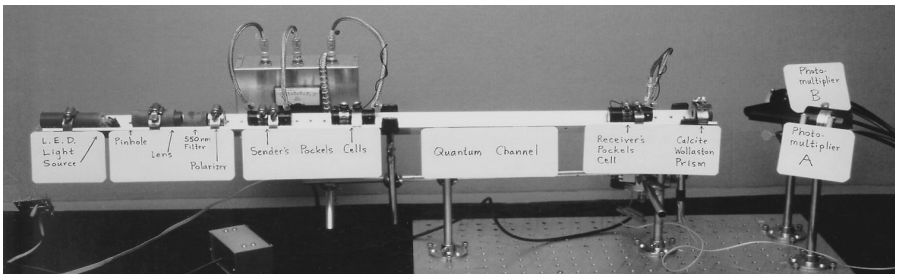

Рис. 32. Перша експериментальна установка КРК BB84

У BB84, як і в більшості протоколів з одиничними поляризованими фотонами, використовуються чотири поляризовані стани фотонів (0º, 45º, 90º, 135º), що передаються квантовим каналом зв'язку. Пошук та виправлення помилок виконується з використанням відкритого класичного каналу, який не повинен бути конфіденційним, тільки автентифікованим. Для виявлення факту дій зловмисника використовується процедура контролю помилок, а для забезпечення теоретико-інформаційної стійкості використовується класична процедура підсилення секретності. Протокол BB84 можна назвати родоначальником протоколів квантової криптографії, яких на сьогодні запропоновано вже кілька десятків. Ефективність протоколу BB84 з кубітами в ідеальних умовах дорівнює 50%. Під *ефективністю у квантовій криптографії* (зокрема у КРК) розуміють відношення

кількості фотонів, що використовуються для генерації ключа до загальної кількості переданих фотонів. Крім того, на сьогодні 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. Вихідними даними КРК є ключова послідовність, яка може бути використана для подальшого шифрування даних. До вищезгаданого типу протоколів КРК (див. рис. 2.4.2) крім BB84 відносяться також протоколи: з шістьома станами, «4+2», Гольденберга-Вайдмана та Коаші-Імото.

Протокол з шістьома станами передбачає використання чотирьох станів, аналогічних протоколу BB84, і додатково вводяться ще два можливих напрямки поляризації – правоциркулярний 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, вже запропоновано *узагальнення протоколу з шістьома станами на багаторівневі квантові системи.* Цей протокол має дещо більшу інформаційну місткість та значно більшу стійкість до атаки «перехоплення – повторної посилки» кудитів. Стійкість протоколу до загальної некогерентної атаки практично така ж, як і протоколу BB84 з кудитами.

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 цього 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.

Крім протоколів з поляризаційним кодуванням також існують і *протоколи КРК з використанням фазового кодування.* Найвідомішим представником цього типу протоколів є *B92* – концептуально найпростіший квантовий протокол, у 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 важливим протоколом для практичних

систем.

Протокол Екерта (він же E91) відноситься до КРК з *використанням переплутаних станів*. Під час передавання інформації за протоколом E91 перехоплення одного із фотонів пари не дає зловмиснику ніякої корисної інформації (лише дозволяє виявити факт появи порушника). Крім того, запропоновано *узагальнення схеми Екерта на тривимірні, та багатовимірні квантові системи,* що значно збільшує інформаційну місткість протоколу.

Протокол SARG04 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 у цих протоколах після квантової передачі. Таке удосконалення дозволяє підвищити стійкість протоколу до атаки розділення кількості фотонів. 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, цьому 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 автентифікації користувачів на таких протоколах не можливо побудувати завершене повноцінне рішення проблеми розподілення криптографічних ключів.

Переваги протоколів КРК: 1) дозволяють завжди виявити атаку пасивного перехоплення (Eavesdropping), так як підключення зловмисника вносить до каналу значно більший рівень помилок порівняно з природнім рівнем; 2) безумовна (теоретико-інформаційна) безпека, що дозволяє використати абсолютно секретний ключ для подальшого шифрування відомими класичними криптосистемами – це відповідно збільшить рівень захищеності суто класичних систем (також можливий синтез КРК з шифром Вернама, що в поєднані зі стійкою схемою автентифікації дасть абсолютно стійку систему обміну повідомленнями).

Недоліки: 1) система, побудована на КРК не може слугувати повноцінним завершеним рішенням (без попередньої автентифікації користувачів) проблеми розподілу ключів; 2) обмеження довжини квантового каналу, тобто неможливість підсилення без втрати квантових властивостей; 3) швидкість передачі інформації квантовим каналом суттєво зменшується зі збільшенням довжини каналу і на відстанях порядку 100 км дорівнює декільком бітам за секунду – для сучасних ІКС це дуже мало; 4) проблеми реєстрації фотонів – ефект «темнового шуму» («темнових відліків»); 5) залежність каналу від зовнішнього впливу (наприклад, від погодних умов, середовища тощо); 6) складність технічної реалізації

протоколів з багатовимірними квантовими системами; 7) деполяризація фотонів (неможливість підсилення за допомогою повторювачів, як у класичних системах); 8) висока ринкова ціна комерційних рішень, що робить їх недоступним, зокрема, для більшості вітчизняних потенційних користувачів.

Квантовий прямий безпечний звязок

Іншим квантовим методом захисту інформації є КПБЗ, характерною особливістю якого є відсутність криптографічних перетворень (відповідно відсутня і проблема розподілу ключів шифрування). Протоколи КПБЗ можна поділити на чотири типи: пінг-понг протокол (різні його варіації), протоколи з передаванням переплутаних кубітів блоками, протоколи з одиничними кубітами та протоколи з групами переплутаних кудитів. Більшість запропонованих до теперішнього часу протоколів КПБЗ потребують передачі кубітів блоками – це дозволяє виявити прослуховування квантового каналу до початку передачі самого повідомлення й таким способом гарантувати безпеку передачі (якщо прослуховування виявлене до передачі повідомлення, то легітимні сторони переривають сеанс і ніяка інформація не витікає до зловмисника). Але для зберігання таких блоків кубітів необхідна квантова пам'ять великого об'єму. Технологія квантової пам'яті активно розробляється, але поки ще далека від масового застосування в стандартному телекомунікаційному встаткуванні. Тому, з точки зору технічної реалізації, перевагу мають протоколи, у яких передача здійснюється одиничними кубітами або невеликими їхніми групами (за один цикл протоколу). Таких протоколів існує не так небагато, і вони мають тільки *асимптотичну безпеку,* тобто атака буде виявлена з високою ймовірністю, але до цього зловмисник зможе одержати деяку частину повідомлення. Отже, виникає проблема підсилення безпеки таких протоколів, тобто створення таких методів попередньої оброблення передаваної інформації, які зроблять перехоплену зловмисником інформацію даремною для нього.

Одним із протоколів КПБЗ, який не потребує квантової пам'яті великого об'єму, є *пінг-понг протокол*. У своєму початковому варіанті протокол використовує *переплутані пари кубітів (ЕПР-пари)* і дозволяє передати один біт класичної інформації за один цикл протоколу. Використання квантового надщільного кодування дозволяє передати два біти за цикл протоколу. Подальше збільшення інформаційної місткості можливе шляхом використання замість переплутаних пар кубітів їх *трійок, четвірок і т.д.*, що перебувають у *переплутаних станах ГХЦ.* Інформаційна місткість пінг-понг протоколу із ГХЦ-станами дорівнює n бітів на цикл, де n – кількість кубітів у використовуваних ГХЦ-станах. Інший шлях підвищення інформаційної місткості пінг-понг протоколу – це використання переплутаних станів багаторівневих квантових систем. На рис. 33 зображено стек протоколів КПБЗ на основі пінг-понг протоколу (включаючи додаткові протоколи стиснення, підсилення стійкості та виправлення помилок):

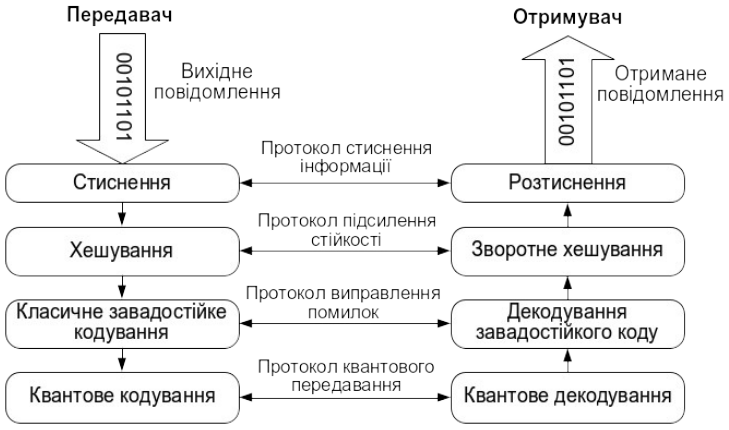

Рис. 33. Стек протоколів КПБЗ на базі пінг-понг протоколу

Крім *режиму передавання повідомлення* у пінг-понг протоколі передбачено також *режим контролю підслуховування,* який призначений для виявлення атаки пасивного перехоплення. Проте, як уже зазначалось, використання цього режиму забезпечує тільки асимптотичну стійкість різних варіантів пінг-понг протоколу. Для підсилення стійкості протоколу необхідно використовувати відповідно допоміжні класичні процедури.

Переваги протоколів КПБЗ: 1) відсутність необхідності у розподіленні секретних ключів (так як відсутній процес шифрування в оригінальних протоколах); 2) можливість обміну інформацією більш ніж між двома користувачами і центром (бродкастінг); 3) можливість виявлення атаки зловмисника; 4) забезпечення високого рівня захищеності (аж до теоретико-інформаційної безпеки) для протоколів з передаванням кубітів блоками. Недоліки: 1) висока ймовірність замаскованої атаки на пінг-понг протокол у квантовому каналі з шумом; 2) складність практичної реалізації систем на основі КПБЗ (аналогічно КРК з кудитами); 3) невисока швидкість передачі кубітів; 4) потреба у квантовій пам'яті великого обсягу для всіх учасників сеансу зв'язку (це здебільшого стосується протоколів з передаванням кубітів блоками); 5) асимптотична безпека пінг-понг протоколу (яка однак може бути підсилена, наприклад, методами класичної криптографії); 6) вразливість до атаки «людина посередині», як і протоколи КРК (хоча ця атака може бути нейтралізованою шляхом автентифікації всіх передаваних у класичному каналі повідомлень).

Інші квантові методи захисту інформації

Зважаючи на невелику кількість фундаментальних досліджень, до менш популярних методів можна віднести протоколи КРС, КПШ, КЦП та квантової стеганографії. Переважна частина квантових протоколів ***КРС*** використовує властивості переплутаних квантових станів. Перший КРС був запропонований Hillery, Buzek та Berthiaume у 1998 р., який, аналогічно деяким протоколам КПБЗ, використовує ГХЦ-триплети (четвірки) кубітів. Цей протокол дозволяє відправнику розділити своє повідомлення між двома (трьома) абонентами таким чином, що вони зможуть його прочитати тільки діючи спільно. Крім того, існують *напів-квантові* протоколи КРС – це *протоколи, що ґрунтуються на рендомізації* і

протоколи, що ґрунтуються на «вимірюванні – повторній відправці» кубітів. Усі протоколи КРС є захищеними, як проти зовнішнього зловмисника, так і проти нечесних дій учасників протоколу. На відміну від класичних схем розділення секрету, квантові та напів-квантові схеми дозволяють виявити підслуховування та не потребують шифрування повідомлень. Найзначнішим недоліком більшості КРС є потреба у наявності великої квантової пам'яті в усіх сторін, що, як уже зазначалося, поки знаходиться за межами можливостей сучасних технологій.

КПШ передбачає шифрування даних подібно до класичних потокових шифрів, але із застосуванням квантового шумового ефекту і може використовуватись в оптичних ІКС. КПШ базується на протоколі *Yuen 2000 (Y-00),* який ще *називають αη-схема.* Вихідними даними передавача у цій схемі є послідовність когерентних станів, що переносить інформацію про дані чи ключ. Теоретико-інформаційна стійкість протоколу Y-00 забезпечується рендомізацією, що базується на квантовому шумі, а також на додаткових математичних (обчислювальних) схемах. Цей протокол має високу швидкість шифрування даних та володіє ідеальною кореляційною захищеністю (стійкий до швидких кореляційних атак). Іншою перевагою КПШ є більша захищеність порівняно із звичайними потоковими шифрами (завдяки квантовому шумовому ефекту і неможливості клонування квантових станів). Що стосується недоліків КПШ, то варто відмітити, перш за все, складність практичної реалізації системи.

КЦП може бути реалізований на *протоколах з одиничними фотонами* та *з переплутаними станами* (автентичний КЦП, оснований на квантових кореляціях ГХЦ). КЦП базується на фундаментальних принципах квантової фізики і полягає у використанні односторонньої функції, яка, на відміну від класичної, є більш захищеною з теоретико-інформаційної точки зору (тобто її захищеність не залежить від потужності обладнання зловмисника – забезпечується теоретико-інформаційна безпека). *Квантова одностороння функція* визначається такими властивостями квантових систем: 1) на відміну від класичних бітів, кубіти можуть існувати у суперпозиціях; 2) згідно теореми Холево кількість класичної інформації, яку можна отримати із квантового стану, є обмеженою (обчислення і перевірка функції не є складними але зворотне обчислення є неможливим). У системах, що використовують КЦП, ідентифікація користувачів та цілісність інформації забезпечується аналогічно класичному ЕЦП. До основних переваг КЦП варто віднести теоретико-інформаційну захищеність та спрощену систему розподілу ключів. Головним же недоліком є можливість генерування обмеженої кількості копій відкритого ключа, крім того, на відміну від ідеальної класичної односторонньої функції, завжди є витік певної кількості інформації про вхідні дані квантової необернеої функції.

Квантова стеганографія аналогічно класичній має за мету приховання самого факту передачі інформації. Усі існуючі моделі систем квантової стеганографії використовують властивості переплутаних станів. Теоретичні дослідження у щодо систем квантової

стеганографії ще не вийшли на рівень практичного застосування, тому важко говорити про їх переваги і недоліки і порівнювати з класичними системами квантової стеганографії.

Комерційні системи квантової криптографії

Першим у світі комерційним рішенням квантової криптографії була система *QPN Security Gateway (QPN-8505),* запропонована компанією MagiQ Technologies (США). Ця система (рис. 34) є економічно вигідним криптографічним рішенням, зорієнтованим на урядові та фінансові організації. У цій системі пропонується захист VPN за допомогою КРК (до ста 256 бітних ключів у секунду на відстань до 140 км) та інтегрованого симетричного шифрування. Система QPN-8505 використовує такі протоколи: квантовий BB84, класичні 3DES (112 біт) та AES (256 біт).

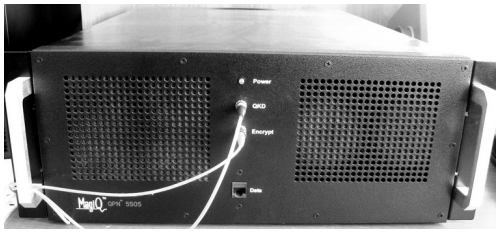

Рис. 34. Квантова криптосистема QPN-8505

За допомогою цієї системи можна організувати захищену квантову ІКС, як це показано на рис. 35. Варто також відзначити, що система QPN Security Gateway є досить дорогою (мінімальна конфігурація системи коштує близько € 80 тис. на серпень 2013 р.).

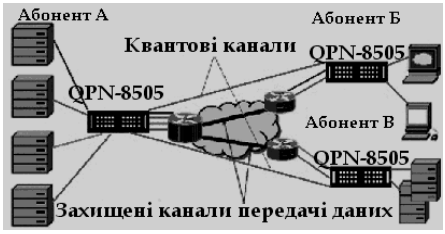

Рис. 35. Варіант організації захищеної квантової ІКС на базі QPN-8505

Сьогодні в Україні подібні системи відсутні і в науково-дослідних інститутах, і в потенційних споживачів такого продукту. Дещо краща ситуація у східних сусідів – один екземпляр криптосистеми від MagiQ Technologies представлений у науково-дослідній лабораторії квантової криптографії Таганрозького кампусу «Південного федерального університету». Крім того, у цій лабораторії є й інше обладнання, придатне для проведення практичних експериментів щодо КРК, випробування стійкості квантових криптосистем тощо. Зокрема, система квантового розподілу ключів *Clavis*^{2} (рис. 36) від швейцарської компанії ID Quantique.

Рис. 36. Швейцарська квантова криптосистема Clavis^2

Система Clavis^2 побудована на автокомпенсуючій оптичній платформі, завдяки чому забезпечується стабільність і низький рівень квантових помилок, що підтверджено численними експериментами. За допомогою цієї системи можна здійснювати захищений розподіл ключів шифрування між двома абонентами на відстань до 100 км. Ринкова вартість системи Clavis2 станом на серпень 2013 р. складає близько € 100 тис., включаючи річну підтримку по телефону та електронній пошті, а також двотижневе навчання інструкторів на базі виробника. Крім того, компанія ID Quantique пропонує й іншу квантову систему під назвою *Cerberis,* що являє собою сервер з автоматичним створенням і секретним обміном ключами захищеним оптоволоконним канал (FC-1G, FC-2G та FC-4G). Ця система (рис. 37) може розподіляти криптографічні ключі на відстань до 50 км, її характерною особливістю є 12 паралельних криптообчислень, що значно підвищує швидкодію. Система Cerberis використовує для шифрування протокол AES (256 біт), а для КРК – протоколи BB84 та SARG (орієнтовна вартість такої системи € 70 тис.).

Рис. 37. Система квантової криптографії Cerberis

Крім того, британська компанія Toshiba Research Europe Ltd (м. Кембрідж) пропонує свою систему КРК під назвою *Quantum Key Server*. Ця система відрізняється простотою своєї архітектури та забезпечує генерацію до ста 256 бітних ключів у секунду та їх односторонню передачу від передавача до приймача. До її складу входить інтегрований модуль автоматичного управління, що проводить неперервний моніторинг системи Quantum Key Server і регулює оптичні характеристики. Інша британська компанія QinetiQ створила першу у світі комп'ютерну мережу, що використовує квантову криптографію – *Quantum Net (Qnet)*. Максимальна довжина ліній зв'язку цієї мережі становить 120 км, та найголовнішим є те, що система Qnet – це перша квантово-криптографічна система, що використовує більше 2 серверів (їх у цій системі аж 6 і всі вони є інтегрованими в Internet).

Вчені провідних країн світу приймають активну участь у реалізації прикладних міжнародних проектів, таких як *SECOQC (Secure Communication based on Quantum*

Cryptography), EQCSPOT (European Quantum Cryptography and Single Photon Technologies) та *SwissQuantum*. Що стосується першого проекту, то ще у далекому 2004 р. Євросоюз вирішив інвестувати € 11 млн. на розвиток квантової криптографії для протидії шпигунським діям американської системи збору інформації ECHELON. Проект стартував у Відні восени 2008 р., його основною метою є виведення квантової криптографії на рівень промислового застосування. Основними завданнями, що вирішуються в межах цього проекту, є створення захищеного середовища вільного ключового обміну, розробка архітектурних компонентів та ПЗ для квантово-криптографічних систем, а також донесення отриманих результатів до широкого кола читачів (користувачів подібних систем та потенційних клієнтів). Базовою задачею проекту SwissQuantum є демонстрація можливостей квантово-криптографічної ІКС і, хоча це не перша система такого роду, проте це перша система, що працює в реальних умовах і з реальним мережевим трафіком. Крім того, по усьому світу інтенсивно ведуться дослідження щодо розробки квантових криптосистем відомими науково-дослідними інститутами та центрами – Institute for Quantum Optics and Quantum Information, Northwestern University, SmartQuantum, BBN Technologies of Cambridge, TREL, NEC, Mitsubishi Electric, ARS Seibersdorf Research, Los Alamos National Laboratory та ін. Що стосується України, то теоретичні дослідження проводяться групами вчених у Національному авіаційному університеті, НТУУ «КПІ», Одеській національній академії зв'язку ім. О.С. Попова та Інституті фізики НАН України. Ці дослідження, в основному, зорієнтовані на розробку нових протоколів квантової криптографії, методів підсилення секретності існуючих протоколів, а також на моделювання процесів передачі (та перехоплення) інформації квантовими каналами з шумом.

Контрольні запитання

1) Поняття та принципи квантової криптографії.

2) Які існують квантові технології захисту інформації?

3) За якими базовими ознаками можна класифікувати методи квантової криптографії?

4) Які є протоколи КРК? Їх переваги, недоліки та перспективи практичної реалізації.

5) Які є протоколи КПБЗ? Їх переваги, недоліки та перспективи практичної реалізації.

6) Порівняйте КРС, КПШ, КЦП та квантову стеганографію з їх класичними (традиційними) аналогами.

7) Які існують комерційні системи квантової криптографії та на базі яких протоколів (розподілу ключів та шифрування) вони побудовані?

8) Назвіть найбільш масштабні міжнародні проекти у галузі квантової криптографії.

9) Пінг-понг протокол КПБЗ: принцип роботи, режими та стійкість.

10) У чому полягає основна перевага квантових засобів захисту інформації над традиційними?

Тема 10. Захист інформаційних ресурсів на базі вітчизняних та міжнародних стандартів

Стандартизація у галузі інформаційної безпеки. Головним завданням стандартів інформаційної безпеки є узгодженість позицій та запитів виробників, споживачів і аналітиків класифікаторів продуктів ІТ. Кожна з категорій фахівців оцінює стандарти та вимоги і критерії, які в них існують, за своїми особистими параметрами. Для споживачів найбільшу роль відіграє простота критеріїв та однозначність параметрів вибору захищеної системи, а для найбільш кваліфікованої частини споживачів – гнучкість вимог та можливість їх застосування до специфічних ІТ-продуктів та середовища експлуатації. Виробники продуктів та послуг, в свою чергу, потребують від стандартів максимальної конкретності та спільних вимог і критеріїв з сучасними прогресивними технологіями

Фахівцям у галузі інформаційної безпеки сьогодні майже неможливо обійтися без знань відповідних стандартів і специфікацій. На це є декілька причин. Формальна причина полягає у тому, що необхідність дотримання певних стандартів закріплена законодавчо. Також, є більш переконливі причини: по-перше, стандарти і специфікації – одна з форм накопичення знань (насамперед на процедурному і програмно-технічному рівнях інформаційної безпеки). У них зафіксовані апробовані, високоякісні рішення та методології, розроблені найбільш кваліфікованими фахівцями; по-друге, і ті, і інші є основним засобом забезпечення взаємної сумісності апаратно-програмних систем та їх компонентів. По відношенню до України можна виділити *міжнародні* та *державні* стандарти у галузі інформаційної безпеки. Крім того, у банківській галузі (яка беззаперечно є найрозвинутішою, з точки зору інформаційної безпеки, у нашій державі) прийняті *галузеві* стандарти.

Міжнародні стандарти. До міжнародних відносяться стандарти серії *ISO/IEC, NIST, ANSI* (стандарти присвячені криптографічним алгоритмам і їх застосуванню у банківських системах), *ITU* (стандарти у галузі телекомунікаційних систем та мереж), стандарти *ITIL, Cobit* та ін. У певній мірі до міжнародних відносяться американські *(FIPS)* та британські стандарти *(BS)*.

Стандарти ISO. У серії ISO27k на сьогодні опубліковано такі стандарти (низка інших готується до публікації найближчим часом):

ISO/IEC 27000:2012 Information technology — Security techniques — Information security management systems — Overview and vocabulary. Цей стандарт містить огляд та словник термінів, що відносяться до СУІБ. Огляд стандартів серії ISO27k показує яким чином необхідно використовувати ці стандарти для планування, впровадження, сертифікації та експлуатації СУІБ. Словник (глосарій) містить ретельно сформульовані формальні дефініції більшості базових термінів, пов’язаних з інформаційною безпекою, що використовуються у

стандартах ISO27k.

ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. Стандарт містить вимоги у галузі інформаційної безпеки щодо створення, розвитку і підтримки СУІБ. У ньому описані кращі світові практики в галузі управління інформаційною безпекою. ISO 27001 встановлює вимоги до СУІБ для демонстрації здатності організації захищати свої інформаційні ресурси. Основою стандарту є система управління ризиками, пов'язаними з інформацією (така система дозволяє визначити на якому конкретно напрямі інформаційної безпеки потрібно зосередити увагу та скільки часу і коштів можна витратити на певне технічне рішення для захисту інформації).

ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls. До 2007 р. цей стандарт називався ISO/IEC 17799 (опублікований у 2000 р., фактично копія Британського стандарту BS 7799-1:1999). Стандарт ISO 27002 висвітлює найкращі практичні поради щодо менеджменту інформаційної безпеки для тих, хто відповідає за створення, реалізацію або обслуговування СУІБ.

ISO/IEC 27003:2010 Information technology — Security techniques — Information security management system implementation guidance. У цьому стандарті розглядаються найважливіші аспекти, необхідні для успішної розробки та впровадження СУІБ відповідно до стандарту ISO 27001. У ньому описується процес визначення і розробки СУІБ від запуску до складання планів впровадження, також описується процес отримання схвалення керівництвом впровадження СУІБ, визначається проект впровадження СУІБ. Крім того, представлені рекомендації щодо планування проекту СУІБ, у результаті якого виходить кінцевий план впровадження СУІБ.

ISO/IEC 27004:2009 Information technology — Security techniques — Information security management — Measurement. Стандарт містить рекомендації щодо розробки та використання вимірювань і мір вимірювання для проведення оцінки ефективності реалізованої СУІБ, а також заходи і засоби контролю та управління відповідно до ISO 27001.

ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management. Цей стандарт забезпечує рекомендації щодо менеджменту ризиків інформаційної безпеки в організації відповідно до стандарту ISO 27001. Однак, цей стандарт не визначає конкретної методології для менеджменту ризиків інформаційної безпеки. Він призначений для визначення в організації підходу до менеджменту ризиків в залежності, наприклад, від галузі діяльності СУІБ, галузі застосування менеджменту ризиків або певного сектору промисловості.

ISO/IEC 27006:2011 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems. Стандарт ISO 17021 встановлює критерії для органів, що здійснюють аудит і сертифікацію систем управління організацій. Якщо ці органи повинні бути акредитовані, як відповідні стандарту ISO 17021, з метою проведення аудиту та сертифікації СУІБ відповідно до ISO 27001, то необхідні

додаткові вимоги та керівництва до ISO 17021. Вони представлені саме у цьому стандарті.

ISO/IEC 27007:2011 Information technology — Security techniques — Guidelines for information security management systems auditing. Цей стандарт є керівництвом щодо управління програмами аудиту СУІБ та проведення внутрішніх і зовнішніх аудитів відповідно до вимог стандарту ISO 27001.

ISO/IEC TR 27008:2011 Information technology — Security techniques — Guidelines for auditors on information security management systems controls. Цей стандарт є керівництвом для всіх аудиторів СУІБ. Він підтримує процес управління ризиками інформаційної безпеки, а також внутрішні, зовнішні та сторонні аудити СУІБ, пояснюючи зв'язок між СУІБ елементів управління, що її підтримують. Крім того, цей стандарт підтримує організації, що використовують ISO 27001 та ISO 27002 у якості стратегічної платформи для управління інформаційною безпекою.

ISO/IEC 27010:2012 Information technology — Security techniques — Information security management for inter-sector and inter-organisational communications. Стандарт надає керівництво із взаємодії і зв'язку щодо інформаційної безпеки між галузями одного сектору промисловості, у різних галузях промисловості і з урядами, а також у період кризи і для захисту критичної інфраструктури чи для взаємного визнання в нормальних умовах ведення бізнесу відповідно до договірних чи інших зобов'язань.

ISO/IEC 27011:2008 Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002. Це керівництво щодо СУІБ у галузі телекомунікації було розроблено спільно з ITU і ідентично за текстом стандарту ITU-T X.1051. Прийняття цього стандарту дозволить телекомунікаційним організаціям забезпечити базові вимоги щодо управління інформаційною безпекою (конфіденційність, цілісність, доступність).

ISO/IEC 27013:2012 — Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 & ISO/IEC 20000-1. Цей стандарт є керівництвом щодо впровадження інтегрованих інформаційної безпеки та управління IT-послугами, на основі як ISO 27001 і ISO 20000-1 (управління IT-послугами специфікації, отримані з ITIL) – дві системи управління, які доповнюють і підтримують одна одну.

ISO/IEC 27014:2013 — Information technology — Security techniques — Governance of information security. Цей стандарт є керівництвом щодо створення концепції і принципів управління інформаційною безпекою, за допомогою яких організації (різних типів і розмірів) можуть оцінити, корегувати, контролювати діяльність організації щодо інформаційної безпеки.

ISO/IEC TR 27015:2012 — Information technology — Security techniques — Information security management guidelines for financial services. Стандарт забезпечує керівництво щодо впровадження інформаційної безпеки та управління нею відповідно до ISO 27002. Він зорієнтований на розробку, реалізацію, підтримку і покращення інформаційної безпеки в

організаціях, що надають фінансові послуги.

ISO/IEC TR 27019:2013 — Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry. Стандарт надає керівні принципи на базі ISO 27002 для управління інформаційною безпекою систем управління технологічними процесами, які використовуються у галузі енергетики. Метою цього стандарту розширення стандартів серії ISO 27000 щодо систем управління технологічними процесами, які використовуються у галузі енергетики, і можливість створення відповідних СУІБ.

ISO/IEC 27031:2011 Information technology — Security techniques — Guidelines for information and communications technology readiness for business continuity. Цей стандарт містить концепції та принципів щодо застосування інформаційно-комунікаційних технологій для забезпечення безперервності бізнесу. Стандарт пропонує структури та фреймворки (набори методів і процесів) для будь-якох організацій – приватних, урядових і неурядових. Визначає критерії та оцінки готовності інформаційно-комунікаційних технологій організацій забезпечити безперервність бізнесу.

ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity. Цей стандарт є керівництвом щодо підвищення рівня кібербезпеки у контексті її унікальності та неперетину з іншими доменами безпеки, а саме: з інформаційною безпекою, безпекою приватних мереж, Інтернет-безпекою, безпекою застосунків та захистом критичної інформаційної інфраструктури. У стандарті проводиться огляд базових відомостей (включаючи термінологію) щодо кібербезпеки, наводиться співвідношення кібербезпеки з іншими зазначеними доменами безпеки та загальні принципи інформаційної взаємодії у процесі вирішення актуальних проблем кібербезпеки.

ISO/IEC 27033-1:2009 Information technology — Security techniques — Network security — Part 1: Overview and concepts. Стандарт містить огляд мережевої безпеки і пов’язаних з нею понять. Визначаються та описуються концепції, пов’язані з мережевою безпекою, а також надаються рекомендації щодо управління безпекою мережі. Мережева безпека у цьому стандарті визначається як безпека обладнання, безпека управління діяльністю, пов’язаною з пристроями, застосунками / послугами та кінцевими користувачами, як додаток до безпеки інформації, що передається каналами зв’язку.

ISO/IEC 27033-2:2012. Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security. У цьому стандарті даються практичні рекомендації щодо організації процесів планування, проектування, впровадження та документування мережевої безпеки на підприємствах. Також, наводяться критерії щодо вибору мережевого обладнання певних вендорів і шаблони документів для опису безпеки різних компонентів мережевої архітектури.

ISO/IEC 27033-3:2010 Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues. Цей стандарт

описує загрози, методи проектування і питання управління відповідно до різних мережевих сценаріїв. Для кожного сценарію стандарт забезпечує детальне керівництво щодо протидії загрозам безпеці, безпеки конструкції і питання управління, які є необхідними для усунення пов'язаних ризиків. У деяких випадках у стандарті наводяться посилання на ISO 27033-4 та ISO 27033-6 (які поки є лише драфтами) для уникнення дублювання змісту цих документів. У цілому, цей стандарт спрямований на реалізацію мережевої безпеки у будь-яких організаціях.

ISO/IEC 27033-5:2013 Information technology — Security techniques — Network security — Part 5: Securing communications across networks using Virtual Private Networks (VPNs). Стандарт дає керівні принципи відбору, реалізації та моніторингу технічного контролю, що необхідно для забезпечення мережевої безпеки за допомогою технології VPN (забезпечення захищених з'єднань усередині мережі та безпечні підключення віддалених користувачів).

ISO/IEC 27034-1:2011 Information technology — Security techniques — Application security — Part 1: Overview and concepts. Стандарт забезпечує керівництво для допомоги організаціям щодо інтеграції засобів захисту в процесах, що використовуються для управління своїми застосунками. Зокрема, він містить визначення понять, принципи і процеси щодо розробки різного роду застосунків та забезпечення їх захисту.

ISO/IEC 27035:2011 Information technology — Security techniques — Information security incident management. Цей стандарт замінив свого попередника ISO 18044, що був чинним з 2004 р. Він встановлює рекомендації щодо менеджменту інцидентів інформаційної безпеки і стосується керівників підрозділів з інформаційної безпеки, інформаційних систем, сервісів та мереж. У стандарті ISO 27035 висвітлено структурний підхід до: виявлення, звітування та оцінки інцидентів інформаційної безпеки; реагування та керування інцидентами інформаційної безпеки; виявлення, оцінювання та управління уразливостями інформаційної безпеки; постійного поліпшення стану інформаційної безпеки та процесу управління інцидентами у результаті управління інцидентами та вразливостями.

ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. Стандарт містить рекомендації для конкретних видів діяльності щодо роботи з цифровими доказами (зокрема, виявлення, збір, придбання і збереження цифрових фактів, які можуть мати доказове значення). Він містить рекомендації для різноманітних ситуацій, що виникають у процесі цифрової оброблення даних і допомагає організаціям щодо їх дисциплінарних процедур та сприяє обміну потенційними цифровими доказами між різними юрисдикціями.

Крім серії ISO27k варто виділити такі ***міжнародні стандарти:***

ISO/IEC 10118 Information technology — Security techniques — Hash-functions (Parts 1-4). Стандарт містить відомості щодо геш-функцій і особливостей їх застосування для забезпечення інформаційної безпеки. Зокрема, у *першій частині* представлені загальні відомості щодо застосування геш-функцій, *друга* – присвячена геш-функції із використанням

n-бітного блокового шифру, *третя* містить опис спеціалізованих геш-функцій, а *четверта* описує геш-функції із використанням модульної арифметики.

ISO/IEC 11770 Information technology — Security techniques — Key management (Parts 1-4). Стандарт пов'язаний з управлінням ключами шифрування – *перша його частина* визначає загальну модель управління ключами (не залежно від використання будь-якого конкретного криптографічного алгоритму); *друга частина* стандарту визначає 13 механізмів формування спільних секретних ключів із використанням симетричної криптографії; *третя* визначає механізми управління ключами на основі асиметричних криптографічних методів; *остання частина* визначає основні механізми створення ключів на основі слабких секретів.

ISO/IEC 15408 Information technology — Security techniques — Evaluation criteria for IT security (Parts 1-3). *Перша частина* стандарту встановлює загальну концепцію та принципи оцінювання інформаційної безпеки, *друга* – визначає зміст і форму представлення функціональних вимог безпеки, що підлягають оцінюванню (містить повний каталог функціональних компонентів, що відповідає сучасним потребам ринку). *Третя* ж частина визначає вимоги довіри з критеріїв оцінювання – включає в себе оцінку рівнів гарантії, які визначають шкалу для вимірювання компонентів для забезпечення завдань оцінювання, а також містить критерії оцінювання профілів захисту та безпеки об'єктів.

ISO/IEC 18028-3:2005 Information technology — Security techniques — IT network security — Part 3: Securing communications between networks using security gateways. Загальною метою усіх частин стандарту ISO 18028 є розширення керівництва щодо IT-безпеки, яке міститься в ISO 13335. Стандарт містить детальний опис конкретних операцій і механізмів, необхідних для реалізації мережевих гарантій безпеки і контролю у широкому діапазоні мережевих середовищ (забезпечуючи зв'язок між загальними питаннями управління IT-безпекою та мережевою безпекою). *Третя ж частина стандарту (ISO 18028-3)* містить, зокрема, огляд шлюзів безпеки за рахунок опису різних архітектур. У ньому викладено методи використання шлюзів безпеки для аналізу мережевого трафіку. Зокрема, це використання фільтрації пакетів, технології SPI (Stateful Packet Inspection), проксі-серверів, трансляції мережевих адрес тощо.

ISO/IEC 18028-4:2005 Information technology — Security techniques — IT network security — Part 4: Securing remote access. *Четверта частина стандарту ISO 18028* є керівництвом для безпечного використання віддаленого доступу (віддалене підключення комп'ютера або до іншого комп'ютера, або до мережі, за рахунок використання мереж загального користування) і його наслідків для IT-безпеки.

ISO/IEC 18031:2011 Information technology — Security techniques — Random bit generation. Цей стандарт висвітлює концептуальні моделі, загальні поняття та вимоги до конструктивних елементів і елементів систем, що використовуються як ГВП (ГПВП) у галузі криптографії. Відповідно до цього стандарту усі ГВП (ГПВП) диференціюються на дві категорії – детерміновані та не детерміновані (у залежності від вибору джерела ентропії –

фіксованого чи змінного відповідно).

ISO/IEC 18033 Information technology — Security techniques — Encryption algorithms — (Parts 1-4). Стандарт складається з чотирьох частин, у яких визначає певні системи шифрування з метою забезпечення конфіденційності даних. *Перша частина* містить визначення базових понять у галузі криптографічного захисту інформації, опис проблеми розподілу ключів шифрування та диференціювання симетричних і асиметричних шифрів. *Друга частина* стандарту присвячена криптографічним системам з відкритим ключем, *третя* – блоковим, а *четверта* потоковим симетричним шифрам.

ISO/IEC 29100:2011 Information technology — Security techniques — Privacy framework. Цей стандарт забезпечує конфіденційність фреймворків, а також визначає загальну термінологію щодо конфіденційності, базові аспекти оброблення особистої інформації, містить посилання на відомі принципи щодо конфіденційності у галузі інформаційних технологій.

ISO/IEC 29192 Information technology — Security techniques — Lightweight cryptography (Parts 1-4). *Перша частина* цього стандарту містить базові терміни і поняття, які застосовуються у трьох інших його частинах. *Друга частина* визначає два блокових шифри, які відносяться до так званої малоресурсної криптографії – це шифри PRESENT (розмір блоку 64 біти, довжина ключа 80 або 128 біт) та CLEFIA (розмір блоку 128 біт, довжина ключа 128, 192 або 256 біт). У *третій частині* стандарту приведено описи двох генераторів ключових даних для малоресурсних шифрів – Enocoro (ключ 80 або 128 біт) та Trivium (ключ 80 біт). *Четверта частина* визначає три малоресурсні механізми із використанням асиметричних криптографічних методи: a) односторонній механізм аутентифікації на основі дискретних логарифмів на еліптичних кривих; b) механізм перевірки справжності малоресурсного обміну ключами для односторонньої автентифікації і створення сесійного ключа; c) механізм підпису на основі ідентифікації.

Стандарти NIST. У складі американського інституту NIST функціонує Центр з комп'ютерної безпеки (відомий як CSRC), який об'єднує фахівців федеральних служб, університетів, найбільших IT-компаній США і займається публікуванням стандартів і рекомендацій у галузі інформаційної безпеки. Створеним центром CSRC документам присвоюється код 800.

Найвагоміші стандарти та рекомендації NIST:

– *SP 800-28 «Загрози користувачам при використанні активного контенту та мобільного коду»;*

– *SP 800-34 «Планування забезпечення безперервності у федеральних інформа-ційних системах»;*

– *SP 800-37 «Управління ризиками інформаційної безпеки у федеральних інформаційних системах»;*

– *SP 800-40 «Управління оновленнями (апгрейдами) безпеки»;*

– *SP 800-41 «Фаєрволи (міжмережеві екрани) і політики їх застосування»;*

– *SP 800-44 «Забезпечення безпеки публічних Web-серверів»;*

– *SP 800-45 «Безпека електронної пошти»;*

– *SP 800-46 «Забезпечення безпеки при організації віддаленого доступу в мережу організації»;*

– *SP 800-48 «Додаткові заходи безпеки при використанні застарілих протоколів бездротових мереж (WEP, WPA)»;*

– *SP 800-50 «Створення програми підвищення обізнаності у галузі безпеки IT»;*

– *SP 800-58 «Інформаційна безпека VoIP»;*

– *SP 800-61 «Управління інцидентами у галузі інформаційної безпеки»;*

– *SP 800-63 «Аутентифікація в інформаційних системах»;*

– *SP 800-77 «Введення в IPSec»;*

– *SP 800-81 «Впровадження Secure DNS»;*

– *SP 800-83 «Антивірусний захист стаціонарних і мобільних робочих місць співробітників»;*

– *SP 800-84 «Тестування планів безпеки IT»;*

– *SP 800-92 «Керування журналами безпеки»;*

– *SP 800-94 «Системи виявлення / попередження вторгнень (IDS / IPS)»;*

– *SP 800-95 «Розробка безпечних Web-сервісів»;*

– *SP 800-111 «Технології шифрування даних при зберіганні»;*

– *SP 800-113 «Введення в SSL VPN»;*

– *SP 800-114 «Захист пристроїв користувачів при організації віддаленого дос-тупу в мережу організації»;*

– *SP 800-115 «Технічні питання оцінки рівня інформаційної безпеки»;*

– *SP 800-118 «Управління паролями»;*

– *SP 800-119 «Питання безпеки при впровадженні IPv6»;*

– *SP 800-121 «Безпека технології Bluetooth»;*

– *SP 800-124 «Забезпечення безпеки мобільних пристроїв організації»;*

– *SP 800-125 «Забезпечення безпеки при використанні технологій віртуалізації»;*

– *SP 800-127 «Забезпечення безпеки WiMAX»;*

– *SP 800-137 «Моніторинг інформаційної безпеки у федеральних інформаційних системах»;*

– *SP 800-144 «Питання безпеки при використанні публічних хмар»;*

– *SP 800-146 «Хмарні обчислення: огляд технологій, аналіз переваг і недоліків».*

Крім стандартів ISO та NIST особливої уваги заслуговують стандарти ITIL та Cobit:

ITIL (Information Technology Infrastructure Library). Стандарт описує найкращу світову практику організації підприємства чи підрозділу, що надає послуги у сфері IT. Методологічний виклад ITIL дозволяє забезпечити ефективне функціонування IT-служб, задовольнити потреби бізнес-користувачів, забезпечити стабільний і передбачуваний

розвиток ІС підприємства. ITIL публікується як серія книжок, кожна з яких висвітлює певну галузь управління у сфері ІТ. Керуючись рекомендаціями та принципами ITIL, багато приватних та урядових організацій досягли значних успіхів у підвищенні якості своїх ІТ-служб. Найновіша його версія – ITIL v3 – складається із п'яти книг: 1) стратегії сервісів; 2) створення сервісів; 3) підготовка сервісів до операційного використання; 4) використання сервісів; 5) безперервне покращення послуг.

Cobit (**C**ontrol **Ob**jectives for **I**nformation & Related **T**echnology). Стандарт містить низку документів зі стандартами щодо оптимізації управління ІТ (аудитом ІТ та ІТ-безпекою). Стандарт сприяє чіткішій координації дій ІТ-департаменту та керівництва компанії, об'єднує у собі ряд інших стандартів, що дозволяє якісно і на високому рівні отримувати інформацію про стан ІТ та управляти цілями й задачами ІТ. Завдання Cobit полягає у ліквідації розриву між керівництвом компанії, з їх баченням бізнес-целей, та ІТ-департаментом, що здійснює підтримку інформаційної інфраструктури, яка повинна сприяти досягненню цих цілей. У цьому стандарті детально описані цілі і принципи управління, об'єкти управління, чітко визначені всі ІТ-процеси (завдання), що протікають у компанії, і вимоги до них, описаний можливий інструментарій (практики) для їх реалізації. В описі ІТ-процесів також приведені практичні рекомендації щодо управління ІТ-безпекою. Основні чинні **державні стандарти України** у галузі інформаційної безпеки – **ДСТУ** та **ГОСТ** (стандарти, які залишились із радянських часів та перших років незалежності України і використовуються до цього часу):

ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка». Цей стандарт встановлює механізм цифрового підписування, що ґрунтується на властивостях груп точок еліптичних кривих над полями Галуа $GF(2^m)$, та правила застосування цього механізму до повідомлень, що передаються каналами зв'язку та/або обробляються у комп'ютеризованих системах загального призначення.

ГОСТ 34.310:95 «Інформаційні технології. Криптографічний захист інформації. Процеси формування й перевірки електронного цифрового підпису». Цей держстандарт встановлює процедури вироблення і перевірки ЕЦП повідомлень (документів), переданих незахищеними телекомунікаційними каналами загального користування у системах оброблення інформації різного призначення, на базі асиметричного криптографічного алгоритму із застосуванням функції гешування. Впровадження системи ЕЦП на базі цього стандарту забезпечує захист переданих повідомлень від підробки, спотворення і однозначно дозволяє доказово підтвердити підпис особи, яка підписала повідомлення.

ГОСТ 34.311:95 «Інформаційні технології. Криптографічний захист інформації. Функція хешування». Стандарт визначає алгоритм і процедуру обчислення геш-функції для будь-якої послідовності двійкових символів, які застосовуються у криптографічних методах оброблення та захисту інформації, у тому числі для реалізації процедур ЕЦП при передачі, обробленні та зберіганні інформації в автоматизованих системах.

ДСТУ ISO/IEC 14888 «Інформаційні технології. Методи захисту. Цифрові підписи з доповненням» (Частини 1-3). Ґрунтується на алгоритмах і механізмах, заснованих на методах асиметричної криптографії. Існують три основних етапи для кожного асиметричного механізму цифрового підписування, а саме процес: генерування пари ключів, складеної з особистого ключа й відповідного відкритого ключа; використання особистого ключа (підписування); використання відкритого ключа (верифікація підпису). *Перша частина* стандарту (гармонізованого із ISO/IEC 14888) присвячена основним поняттям та положенням, у *другій* розглядаються механізми на основі ідентифікаторів, а в *третій* – механізми на основі сертифікатів (DSA, ECDSA та ін.).

ДСТУ ISO/IEC 9798-1:2002 «Інформаційні технології. Методи безпеки. Автентифікації сутностей» (Частини 1-3). Цей стандарт визначає модель автентифікації і загальні вимоги та обмеження для механізмів автентифікації суб'єктів із використанням методів захисту. Ці механізми використовують для підтвердження того, що суб'єкт є тим, ким він себе заявив. Суб'єкт, який необхідно автентифікувати, доводить свою тотожність показом свого знання таємної інформації. Механізми визначають як обміни інформацією між суб'єктами і, за необхідності, обміни з третьою довірчою стороною. Надання послуг неспростовності знаходиться поза сферою застосування цього ДСТУ.

ДСТУ ISO/IEC 10118-1:2003 Інформаційні технології. Методи безпеки. Геш-функції (Частини 1-3). *Перша частина* стандарту описує геш-функції і, отже, може, бути застосований для забезпечення послуг автентифікації, цілісності та неспростовності. Геш-функції перетворюють довільні рядки бітів у рядки бітів фіксованої довжини, використовуючи означений алгоритм. Їх можна використовувати для: скорочення повідомлення до короткого відбитку, що є вхідною величиною до механізму ЕЦП; прив'язування користувача з заданим рядком бітів, не розкриваючи цього рядка. Геш-функції, представлені у цьому стандарті, не містять в собі використання секретних ключів. Проте, ці геш-функції разом із секретними ключами можуть бути використанні для створення кодів автентифікації повідомлень (забезпечення автентифікацію джерела повідомлень у доповненні до цілісності повідомлення). *Друга частина* визначає чотири геш-функції, які відповідають загальній моделі, наведеній у ISO/IEC 10118-1. У третій частині визначено спеціалізовані геш-функції (спеціально побудовані). Вони базуються на повторному використанні циклової функції. Визначено сім різних циклових функцій, які породжують різні спеціалізовані геш-функції.

ДСТУ ISO/IEC 18014 «Інформаційні технології. Методи захисту. Послуги штемпелювання часу» (Частини 1-3). *Першу частину* стандарту застосовують щоб визначити мету органу штемпелювання часу, описати загальну модель, на якій ґрунтуються послуги штемпелювання часу, визначити послуги та протоколи штемпелювання часу, а також визначити протоколи між залученими об'єктами. *Друга частина* містить опис механізмів, що генерують незалежні токени, а в *третій* увага приділяється зв'язаним токенам.

ДСТУ ГОСТ 28147:2009 «Системи оброблення інформації. Захист криптографічний. Алгоритми криптографічного перетворення». Стандарт встановлює єдиний алгоритм криптографічного перетворення для систем оброблення інформації в мережах ЕОМ, окремих обчислювальних комплексах і ЕОМ, який визначає правила шифрування даних і вироблення імітовставки. Алгоритм криптографічного перетворення призначений для апаратної або програмної реалізації, задовольняє криптографічним вимогам і за своїми можливостями не накладає обмежень на ступінь секретності інформації, що захищається. Стандарт обов'язковий для організацій, підприємств та установ, що застосовують криптографічний захист даних, збережених і переданих в мережах ЕОМ, в окремих обчислювальних комплексах або в ЕОМ. Фактично, він є адаптацією радянського ГОСТ 1989 р.

ДСТУ 3396.0-96 «Захист інформації. Технічний захист інформації. Основні поло-ження». Цей стандарт установлює об'єкт, мету, основні організаційнотехнічні положення забезпечення технічного захисту інформації, неправомірний доступ до якої може завдати шкоди громадянам, організаціям (юридичним особам) та державі, а також категорії нормативних документів системи технічного захисту інформації. Вимоги стандарту є обов'язковими для підприємств та установ усіх форм власності і підпорядкування, громадян – суб'єктів підприємницької діяльності, органів державної влади, органів місцевого самоврядування, військових частин, представництв України за кордоном, які володіють, користуються та розпоряджаються інформацією, що підлягає технічному захисту.

ДСТУ 3396.1-96 «Захист інформації. Технічний захист інформації. Порядок проведення робіт». Цей стандарт установлює вимоги до порядку проведення робіт з технічного захисту інформації. Відповідно до нього, послідовність робіт має Б: 1) проведення обстеження підприємства, установи, організації; 2) розроблення і реалізація організаційних, первинних технічних, основних технічних заходів з використанням засобів забезпечення технічного захисту інформації; 3) приймання робіт з технічного захисту інформації; 4) атестація засобів (систем) забезпечення інформаційної діяльності на відповідність вимогам.

ДСТУ 3396.2-97 «Захист інформації. Технічний захист інформації. Терміни та визначення». Стандарт установлює терміни та визначення понять у сфері технічного захисту інформації. Терміни, регламентовані у цьому стандарті, обов'язкові для використання в усіх видах організаційної та нормативної документації, а також для робіт зі стандартизації, і рекомендовані для використання у довідковій та навчально-методичній літературі, що належить до сфери технічного захисту інформації.

Крім того, у банківській сфері України діють **галузеві стандарти**:

ГСТУ СУІБ 1.0/ISO/IEC 27001:2010 «Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги». Під час адаптації (модифікації) відповідного міжнародного стандарту до цього документу було внесено окремі зміни, зумовлені правовими вимогами і конкретними потребами банківської сфери діяльності. Цей галузевий стандарт створений, в першу чергу, для надання моделі розроблення, впровадження,

функціонування, моніторингу, перегляду, підтримування та вдосконалення СУІБ. Прийняття СУІБ повинне бути стратегічним рішенням для організації. На проектування та впровадження СУІБ організації впливають потреби та цілі організації, вимоги безпеки, застосовувані процеси, розмір і структура організації. За своєю структурою цей стандарт фактично ідентичний міжнародному прототипу.

ГСТУ СУІБ 2.0/ISO/IEC 27001:2010 «Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою». Цей стандарт є модифікацією міжнародного стандарту ISO/IEC 27001, до якого було внесено певні зміни, зумовлені правовими вимогами і конкретними потребами банківської сфери діяльності.

Контрольні запитання

1) Передумови та чинники виникнення стандартів у галузі інформаційної безпеки.

2) Назвіть основні міжнародні організації, які займаються стандартизацією у галузі інформаційної безпеки?

3) Стандарти серії ISO27k: особливості та загальна характеристика.

4) Які із стандартів ISO можна віднести до документів, що регулюють процес захисту інформації в ІКС? Чому?

5) Назвіть основні стандарти та рекомендації NIST.

6) У чому полягають особливості застосування стандарту ITIL?

7) Що являє собою стандарт Cobit?

8) Основні державні стандарти України у галузі інформаційної безпеки.

9) Дайте коротку характеристику державним стандартам України у сфері технічного захисту інформації.

10) Які Ви знаєте вітчизняні галузеві стандарти щодо забезпечення інформаційної безпеки? Передумови їх виникнення.

Глосарій

Аплет (Applet) — коротка комп'ютерна програма, що функціонально розширює можливості основної програми, або інтернет-застосунку (наприклад, додає у веб-сторінку функцію анімації.

Атака (Attack) — заходи, які вживаються зловмисниками для підриву безпеки системи (DoS-атака, одержання НСД тощо).

Автентифікація (Authentication) — процедура перевірки приналежності користувачеві чи процесу користувача права доступу на підставі пред'явленого ним ідентифікатора.

Байт (Byte) — одиниця кількості інформації (частина машинного слова), яка складається з восьми бітів.

Бекдор (Backdoor) — програми, які встановлює зломщик на атакованому ним комп'ютері, після отримання початкового доступу, з метою повторного отримання доступу до системи.

Біометрія (Biometrics) — сукупність автоматизованих методів ідентифікації та автентифікації людей на основі їх фізіологічних і поведінкових характеристик.

Біт (Bit) — мінімальна одиниця кількості інформації, що відповідає одному двійковому розряду («0» або «1»).

Брандмауер Windows (Windows Firewall) — вбудований в ОС Windows міжмережевий екран, що з'явився у версії Windows XP Sp2.

Веб-сервер (Web Server) — це сервер, який приймає HTTP-запити від клієнтів (зазвичай веб-браузерів) і видає їм HTTP-відповіді (зазвичай разом з HTML-сторінкою) зображенням, файлом, медіа-потоком або іншими даними.

Вектор ініціалізації (Initialization Vector) — вектор, що містить початкові значення, необхідні для запуску (наприклад, криптосистеми).

Відбілювання — це процедура XOR даних з підключами перед першим раундом і після останнього раунду. Уперше ця техніка була використана у шифрі Khufu / Khare і, незалежно, R. Rivest у алгоритмі шифрування DESX. J. Killian (NEC) і Ph. Rogaway (Каліфорнійський університет) показали, що відбілювання дійсно ускладнює завдання пошуку ключа повним перебором у DESX.

Віртуальна мережа (Virtual Network) — виділена мережа на базі загальнодоступної мережі, що підтримує конфіденційність переданої інформації за рахунок використання тунелювання та інших процедур захисту.

Вірус (Virus) — програма, яка здатна до багаторазового самовільного створення свого тіла і зазвичай модифікує (заражає) інші програми (записані у файлах чи системних областях) для подальшого створення нового тіла та одержання управління з метою

модифікації записів, знищення файлів, завантаження ресурсів і виконання інших руйнівних впливів у комп'ютерній системі.

Випадкові числа (Random Numbers) — така послідовність чисел, для якої неможливо передбачити наступне число, навіть якщо відомі попередні.

Генератор випадкових послідовностей (Random Numbers Generator) — обчислювальний або фізичний пристрій, для отримання ВП та ПВП, спроектований для генерації послідовності номерів чи символів, які не відповідають будь-якому шаблону.

Гібридна криптосистема (Hybrid Cryptosystem) — криптосистема, основана на асиметричних і симетричних методах криптографії, при цьому криптографічна система з відкритим ключем задіюється тільки для управління загальними ключами, які потім використовуються в криптосистемах із секретним ключем.

Дайджест-автентифікація (Digest Authentication) — автентифікація, при якій пароль користувача передається в гешованому вигляді.

Експлойт (Exploit) — це комп'ютерна програма, фрагмент програмного коду або послідовність команд, що використовують уразливості в ПЗ та призначені для проведення атаки на обчислювальну систему (метою атаки може бути як захоплення контролю над системою (підвищення привілеїв), так і порушення її функціонування (DoS-атака)).

Застосунок (Application) — користувацька комп'ютерна програма, що дає змогу вирішувати конкретні прикладні задачі користувача (наприклад, текстовий процесор, графічний редактор, електронні таблиці, оглядач, поштовий клієнт або медіаплеєр тощо).

Зондування (Probe) — механізм активного аналізу, який дозволяє переконатися у присутності (відсутності) на аналізованому вузлі уразливостей.

Ідентифікація (Identification) — присвоєння особі ідентифікатора (ознака, яка служить для ідентифікації особи чи предмета, що розпізнається) або порівняння ідентифікатора з переліком привласнених ідентифікаторів (наприклад, ідентифікація за штрих-кодом).

Інсайдер (Insider) — співробітник, який використовує свої службові повноваження для доступу до інформації в небажаних для організації цілях (викрадення чи знищення інформації).

Інформаційна безпека (Information Security) — 1) забезпечення конфіденцій-ності, цілісності та доступності інформації; 2) стан захищеності ресурсів інформаційно-комунікаційних (інформаційно-телекомунікаційних) систем, при якому забезпечується їх існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз.

Інформаційно-телекомунікаційна система (Information & Communication System) — це сукупність інформаційних систем, мереж і каналів передачі інформації, засобів комунікації і управління інформаційними потоками.

Квант (Quantum) — елементарна неподільна порція деякої фізичної величини, яка є носієм певного типу взаємодії (наприклад, фотон, фонон, гравітон).

Квантова система захисту інформації (Quantum Information Security System) — система захисту інформації, у якій хоча б одна із задач вирішується за допомогою квантових методів захисту інформації.

Квантовий метод захисту інформації (Quantum Information Security Method) — сукупність теоретичних принципів та практичних прийомів, що використовують властивості квантів, ґрунтуються на непорушності постулатів квантової механіки і спрямовані на забезпечення захищеності базових характеристик інформації.

Ключ шифрування (Encryption Key) — змінюваний елемент шифру, який застосовується для шифрування (зашифрування / розшифруання) конкретного повідомлення.

Кубіт (Qubit, Q-bit) — мінімальна величина квантової інформації (аналогом у класичній інформації є біт), дворівнева квантова система, що, на відміну від класичного біта, може перебувати у стані суперпозиції (тобто приймати значення і «1», і «0» у деякий момент часу з певною ймовірністю). Математично, кубіт є вектором у двовимірному гільбертовому просторі.

Криптосистема (Cryptosystem) — це сукупність алгоритму шифрування, усіх можливих відкритих текстів, шифротекстів і ключів.

Критичні комп'ютерні системи (Critical Computer Systems) — складні комп'ютеризовані організаційно-технічні й технічні системи, блокування або порушення функціонування яких потенційно приводить до втрати стійкості організаційних систем державного управління і контролю, втрати обороноздатності держави, руйнування системи фінансового обігу, дезорганізації систем енергетичного й комунікаційно-транспортного забезпечення держави, а також до глобальних екологічних і техногенних катастроф.

Маска підмережі (Subnet Mask) — число, що додається до IP-адреси для визначення адрес, які є частиною тієї самої підмережі.

Маршрут (Route) — шлях, який використовується для переміщення інфор-мації з одного місця в інше, наприклад, у мережі з комутацією пакетів маршрутом є повний список вузлів мережі (між двома конкретними кінцевими системами), якими цей пакет (чи група пакетів) має пройти чи пройшов.

Маршрутизація (Routing) — 1) процедура, яка використовується для визначення маршруту пакета в мережі з комутацією пакетів; 2) процес пересилання датаграм між маршрутизаторами з метою їх доставки адресату.

Міжмережевий екран (Firewall) — комплекс апаратних чи ПЗ, що здійснює контроль і фільтрацію мережевих пакетів, які проходять через нього на різних рівнях моделі OSI відповідно до заданих правилам. Основним завданням мережевого екрану є захист комп'ютерних мереж або окремих вузлів від НСД. Також, мережеві екрани часто називають фільтрами, так як їх основне завдання – не пропускати (фільтрувати) пакети, що не підходять під критерії, визначені в конфігурації.

Мережа (Network) — середовище передавання, взаємозв'язані ним вузли і необхідне для реалізації цього зв'язку ПЗ, яке призначене для організації розподіленої оброблення інформації.

Нонс (Nonce) — довільне число використовуване під час криптографічного зв'язку лише один раз. Нонс часто є ВП або ПВП, що утворене протоколом автентифікації, для гарантування унеможливлення використання старих сеансів зв'язку в атаці відтворенням. Наприклад, нонс використовує дайджест автентифікація HTTP для обчислення MD5 гешу/дайджесту пароля. З кожною відповіддю 401 сервер породжує новий нонс і відсилає його як частину відповіді клієнту, той, у свою чергу, може відправити серверу його відповідь, включно з нонсом, і також свої логін і пароль. Такий підхід практично унеможливлює атаки відтворенням.

Пароль (Password) — це, як правило, рядок символів, що підтверджує право доступу користувача до ресурсів та його привілеї.

Підмережа (Subnet) — проста широкомовна мережа, у якій не потрібна маршрутизація пакетів між двома комп'ютерами.

Політика міжмережевої взаємодії (Inter-networking Policy) — частина політики безпеки організації, яка визначає вимоги до безпеки інформаційного обміну із зовнішнім середовищем.

Принцип Керкхоффса (Kerckhoffs`s Principle) — принцип, відповідно до якого 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 інформації легше перешкоджати противнику, оскільки міняти їх можна досить часто.

Псевдовипадкова двійкова послідовність (Pseudorandom Binary Sequence) — частковий випадок ПВП, у якому елементи приймають два можливі значення «0» і «1» (інколи цими значеннями є «–1» та «+1»).

Псевдовипадкові числа (Pseudorandom Numbers) — послідовність чисел, яка має властивості ВП, проте кожне наступне число обчислюється за певною формулою.

Система захисту інформації (Information Security System) — сукупність взаємопов'язаних заходів, засобів та методів, спрямованих на розв'язання задач захисту інформації (забезпечення конфіденційності, цілісності та доступності) в умовах впливу загроз природного чи штучного характеру (реалізація яких може завдати шкоди легітимним користувачам та власникам інформації).

Сканери уразливості (Vulnerability Scanners) — програми, які здійснюють пошук уразливостей у системі і можуть бути використані для реалізації мережевих атак.

Сканування (Scanning) — механізм пасивного аналізу, за допомогою якого сканер намагається визначити наявність уразливості без фактичного підтвердження її наявності (за непрямими ознаками).

Сканування портів (Portscanning) — це процес пробного підключення до портів TCP і UDP досліджуваного комп'ютера з метою визначити, які саме служби на ньому запущені і чи обслуговуються ними відповідні порти, що знаходяться в стані очікування запитів.

Словникова атака (Dictionary Attack) —метод зламування системи парольного захисту перебором елементів одного або декількох словників. Для несанкціонованого проникнення у комп'ютерні системи зазвичай використовуються спеціальні ПЗ, що обробляють власні словники користувачів або словникові файли, які зберігаються на сервері або локальних жорстких дисках.

Соціальний інжиніринг (Social Engineering) — загроза інформації, пов'язана з отриманням певних даних (наприклад, імен користувачів, паролів, номерів телефонів тощо) від різних людей, які атакуються за допомогою інформаційного обміну (з урахуванням людського чинника).

Токен (Token) — як правило, фізичний пристрій, що використовується для спрощення автентифікації (наприклад, смарт-карта або USB-ключ).

Тунелювання (Tunneling) — спосіб передачі інформації через проміжну мережу за технологією інкапсуляції. Такою інформацією можуть бути кадри (або пакети) іншого протоколу. При інкапсуляції кадр не передається в згенерованому вузлом-відправником вигляді, а забезпечується додатковим заголовком, містить інформацію про маршрут, що дозволяє інкапсульованим пакетам проходити через проміжну мережу (Інтернет). На кінці тунелю кадри деінкапсулюються і передаються одержувачу.

Фотон (Photon) — квант електромагнітного поля, елементарна нейтральна частинка, що є носієм електромагнітної взаємодії.

Хост (Host) — мережевий комп'ютер, що надає ресурси для виконання обчислень, доступу до бази даних або до спеціальних програм. У багатомашинному комплексі – головний або управляючий комп'ютер, а в Інтернет – комп'ютер з унікальною IP-адресою та ім'ям домену, що виконує функції початкового чи кінцевого вузла передавання даних.

Хробак, черв'як (Worm) — різновид вірусу, який здійснює транспортування свого тіла вузлами обчислювальної мережі.

Шифротекст (Cipher Text) — це дані, представлені у зашифрованій формі і мають прихований семантичний зміст, який утворюється після шифрування (криптографічного перетворення) відкритого тексту (з неприхованим семантичним змістом).

Шифрування (Encrypting) — оборотне перетворення даних з метою приховання змісту інформації, *дешифрування (decrypting)* – зворотній процес, що полягає у відновленні первинних (до шифрування) даних. Проте, у сучасні науковій літературі під *шифруванням* розуміється синтез процесів зашифрування і розшифрування, а от дешифрування – це відновлення вхідного тексту без знання ключа (тобто, це процес злому шифру – криптоаналіз).

Advanced Encryption Standard — симетричний алгоритм блочного шифрування (розмір блока 128 біт, ключ 128/192/256 біт), прийнятий як стандарт шифрування урядом США за результатами конкурсу AES.

Adware (Spyware, Browser, Hijakers) — рекламне ПЗ, призначене для перегляду рекламних повідомлень (найчастіше у вигляді графічних банерів) і перенаправлення пошукових запитів на рекламні сайти.

ARP — мережевий протокол, призначений для перетворення IP-адрес (адрес мережевого рівня) в MAC-адреси (адреси канального рівня) у мережах TCP/IP.

Broadcast — розсилання, яке називається широкомовним повідомленням, і полягає в тому, що якщо у полі номера вузла призначення стоять тільки одиниці, то пакет, що має таку адресу, розсилається всім вузлам мережі із заданим номером мережі.

CCMP — протокол шифрування 802.11i створений для заміни TKIP (обов'язкового протоколу шифрування у WPA і WEP) як надійніший варіант. CCMP є обов'язковою частиною стандарту WPA2, і необов'язковою частиною стандарту WPA.

Cookie — невеликий фрагмент даних, що відправлений веб-сервером і зберігається на комп'ютері користувача, який веб-клієнт (зазвичай веб-браузер) щоразу пересилає веб-серверу в HTTP-запиті при спробі відкрити сторінку відповідного сайту.

Denial of Service Attack (DoS-атака) — атака, спрямована на навмисне усунення чи обмеження можливостей ІКС щодо використання (забезпечування обслуговування), наприклад, уповільнення роботи або блокування доступу до системи, насичення непотрібними даними, перевантаження портів, маніпуляції з ключовими файлами, захоплення ресурсів тощо.

DNS-server — застосунок, призначений для відповідей на DNS-запити з відповідного протоколу.

EAP — розширений протокол ідентифікації, тобто загальний протокол для підтвердження автентичності протоколу PPP, який підтримує кілька механізмів ідентифікації. EAP не обирає певний механізм ідентифікації на етапі керування каналом, а відкладає вибір до етапу ідентифікації – це дозволяє ідентифікатору запитати більше інформації ще до вибору певного механізму.

ESSID — використання системи мережевих ідентифікаторів.

Ethernet — базова технологія локальних обчислювальних (комп'ютерних) мереж з комутацією пакетів, що використовує протокол CSMA / CD (множинний доступ з виявленням колізій). Цей протокол дозволяє у кожний момент часу лише один сеанс передачі в логічному сегменті мережі.

FIN — мітка, яка, будучи встановленою, вказує на завершення з'єднання.

FTP — протокол, призначений для передачі файлів в комп'ютерних мережах і дає можливість абоненту обмінюватися файлами з будь-яким комп'ютером мережі, що підтримує цей протокол.

GET — метод, який використовується для запиту вмісту зазначеного ресурсу.

HTTP — протокол прикладного рівня передачі даних, який дозволяє шифрувати усі дані, передані між браузером і сервером, а не тільки імена користувачів і паролі.

HTTPonly — мітка, що робить cookie недоступними для скриптів з боку клієнта.

IGMP — протокол керування груповою (multicast) передачею даних у мережах, що базуються на протоколі IP.

ICMP — протокол обміну керуючими повідомленнями, який дозволяє маршрутизатору повідомити кінцевому вузлу про помилки, які виникли при передачі будь-якого IP-пакету від цього кінцевого вузла.

Internet Protocol (IP) — найбільш широко розповсюджена реалізація ієрархічної схеми мережевої адресації. Використовуваний в мережі Інтернет, протокол відповідає за адресацію пакетів, але не відповідає за встановлення з'єднань, не є захищеним та надійним і дозволяє реалізувати тільки негарантовану доставку даних.

IP-адреса — ідентифікатор (унікальний числовий номер) мережевого рівня, що використовується для адресації комп'ютерів чи пристроїв у мережах, що побудовані з використанням протоколу TCP/IP (наприклад, Інтернет).

IP спуфінг — вид хакерської атаки, що полягає у використанні чужої IP-адреси з метою обману системи безпеки.

IPSec — набір протоколів для забезпечення захисту даних, переданих за міжмережевим протоколом IP, дозволяє здійснювати підтвердження автентичності та / або шифрування IP-пакетів.

IPv4 — четверта версія мережевого протоколу IP. Перша версія протоколу, яка набула широко розповсюдження, використовує 4-байтну форму запису адрес пристроїв у комп'ютерній мережі.

IPv6 — нова версія IP-протоколу – IP версії 6, що виділяє на адресу 16 байтів (128 біт).

Kerberos — мережевий протокол автентифікації, що дозволяє передавати дані через незахищені мережі для безпечної ідентифікації.

Keyloggers — вид троянських програм, основною функцією яких є перехоплення даних, що вводяться користувачем через клавіатуру. Об'єктами викрадання є персональні і мережеві паролі доступу, логіни, дані кредитних карт та інша персональна інформація.

L2TP — тунельний протокол у комп'ютерних мережах, що використовується для підтримки VPN. L2TP не забезпечує шифрування та конфіденційність сам по собі. Для забезпечення конфіденційності він опирається на інкапсульований протокол.

Limitedbroadcast — розсилання, яке називається обмеженим широкомовним повідомленням, і полягає в тому, що якщо всі двійкові розряди IP-адреси рівні «1», то пакет з такою адресою призначення повинен розсилатися усім вузлам, що перебувають у тій же мережі, що й джерело цього пакета.

Link-state Technology — технологія відстеження стану каналу між двома маршрутизаторами.

Loopback — IP-адреса, перший октет якої дорівнює 127. Використовується для тестування програм і взаємодії процесів у межах одної машини.

Man-in-the-middle Attack — атака, що полягає у здатності зловмисника читати і видозмінювати за своєю волею повідомлення, якими обмінюються легітимні користувачі, причому жоден з останніх не може здогадатися про його присутність в каналі.

MIC — криптографічний контроль суми, призначений для контролю цілісності пакетів та виявлення підробки у бездротових мережах, що перешкоджають зловмиснику змінювати зміст пакетів.

MOSPF — протокол, що дозволяє маршрутизаторам використовувати свої бази даних стану каналу для побудови дерев доставки і подальшої маршрутизації багатоадресного трафіку.

MPLS — механізм високопродуктивної телекомунікаційної мережі, який здійснює передачу даних від одного вузла мережі до іншого за допомогою міток.

Multicast — форма групової IP-адреси, означає, що цей пакет повинен бути доставлений відразу декільком вузлам, які утворять групу з номером, зазначеним у полі адреси.

NIST STS — набір тестів, який використовується для дослідження статистичних властивостей ГВП та ГПВП.

NTLM — протокол мережевої автентифікації, розроблений фірмою Microsoft спеціально для Windows NT.

OAuth — відкритий протокол авторизації, який дозволяє надати третій стороні обмежений доступ до захищених ресурсів користувача без необхідності передавати їй (третій стороні) логін та пароль.

OpenAuth — система автентифікації, аналог OpenID.

OpenID — децентралізована система автентифікації користувачів.

OSPF — протокол динамічної маршрутизації, заснований на технології відстеження стану каналу, що використовує для знаходження найкоротшого шляху Алгоритм Дейкстри.

Pharming — порівняно новий вид Інтернет-шахрайства. Так звані фармінг технології дозволяють змінювати DNS записи або записи у файлі HOSTS. У разі відвідування користувачем легітимної, на його погляд, сторінки проводиться перенаправлення на підроблену сторінку, створену для збирання конфіденційної інформації. Найчастіше такі сторінки підміняють сторінки банків (як офлайнових, так і онлайнових).

Phishing — вид Інтернет-шахрайства, метою якого є отримання доступу до конфіденційних даних користувачів (логінів та паролів).

Ping — утиліта для перевірки з'єднань в мережах на основі TCP / IP, а також повсякденне найменування самого запиту.

Plaintext Attack — атака на криптосистему, основана на тому, що криптоаналітик знає відкритий та зашифрований тексти і йому треба визначити ключ, на якому здійснюється шифрування повідомлень.

POST — метод, який застосовується для передачі даних користувача заданому ресурсу.

Pornware — утиліти, пов'язані із показом користувачам (різних вікових категорій) інформації порнографічного характеру.

PPTP — тунельний протокол типу точка-точка, що дозволяє комп'ютеру встановлювати захищене з'єднання з сервером за рахунок створення спеціального тунелю у стандартній незахищеній мережі. PPTP поміщає (інкапсулює) кадри PPP в IP-пакети для передачі глобальною IP-мережею, наприклад Інтернет.

RADIUS — протокол для реалізації автентифікації, авторизації та збору відомостей про використані ресурси, розроблений для передачі відомостей між центральною платформою та обладнанням.

Riskware — клас ПЗ, до якого належать легальні програми (дякі з них вільно продаютьяс і широко використовуються легально), які в руках зловмисника здатні завдати шкоди користувачеві та його даним.

RIP — протокол маршрутної інформації, один з найпростіших протоколів маршрутизації.

RST — обірвання з'єднання, очищення буфера.

S-box — нелінійна таблиця замін, що використовується у декількох трансформаціях заміни байт і в процедурі розширення ключів для взаємнооднознач-ної заміни значення байту (застосовується, зокрема, у блокових криптоалгоритмах).

SMTP — широко використовуваний мережевий протокол, призначений для передачі електронної пошти в мережах TCP / IP.

Sniffing — атака в мережах, яка ґрунтується на контролі трафіка (за допомогою спеціальних програм – сніферів) визначених ділянок мережі з метою несанкціонованого отримання ідентифікаційної, парольної та іншої інформації.

Spoofing — 1) навмисна спроба змусити користувача або ресурс системи виконати неправильну дію; 2) атака в мережі (з протоколом TCP/IP), коли порушник привласнює IP-адресу, за допомогою якої він обходить мережеву систему захисту або здійснює «маскарад».

SSL — криптографічний протокол, який забезпечує встановлення безпечного з'єднання між клієнтом і сервером. SSL спочатку розроблений компанією Netscape Communications. Згодом, на базі протоколу SSL 3.0 був розроблений і прийнятий стандарт RFC, що отримав ім'я TLS.

SYN — синхронізація номерів послідовності.

TCP / IP — базовий набір протоколів, відповідальний за розбивання вихідного повідомлення на пакети (TCP), доставку пакетів на вузол адресата (IP) і збирання (відновлення) вихідного повідомлення з пакетів (TCP).

TKIP — протокол інтеграції тимчасового ключа (безпосередньо протокол шифрування), який на відміну від протоколу WEP використовує інший механізм генерації ключів, щоправда він заснований на застарілому алгоритмі RC4. Якщо у WEP довжина вектору ініціалізації дорівнює 24 бітам, то в протоколі TKIP використовується 48 біт. Крім того, вектор ініціалізації відбирається не випадково (псевдовипадково) як раніше, а послідовно, до того ж пакети, що прийшли з невірним номером, відкидаються.

Token Ring — «маркерне кільце», архітектура кільцевої мережі з маркерним (естафетним) доступом.

Transmission Control Protocol — один з основних мережевих протоколів Інтернет, призначений для управління передачею даних в мережах і підмережах TCP / IP.

UDP — протокол користувальницьких датаграм – один з ключових елементів Internet Protocol Suite (більш відомого як TCP / IP), набору мережевих протоколів для Інтернет.

UN / EDIFACT — це сформульована певним чином мова подання комерційних документів, яку доцільно використовувати для зв'язку підприємств із зовнішніми організаціями.

Vishing — технологія Інтернет-шахрайства, різновид фішингу, що полягає у використанні зі злими намірами автонабирачів і можливостей Інтернет-телефонії для крадіжки особистих конфіденційних даних, таких як паролі доступу, дані банківських та ідентифікаційних карт тощо.

WEP — алгоритм захисту бездротових мереж стандарту IEEE 802.11. Передавання даних у бездротових мережах виконується за допомогою радіохвиль, отже, порівняно з даними дротових мереж, ці дані легше перехопити. У протоколі WEP не передбачено жодної підтримки механізмів керування ключами доступу. У більшості середовищ одним і тим самим ключем користуються декілька клієнтських вузлів. У середовищах, де ключі не підлягають регулярній зміні, разом з уразливостями WEP це може становити додаткову загрозу. Тому, цей алгоритм захисту вважається застарілим.

Wi-Fi — технологія бездротового обміну даними, що відноситься до групи стандартів IEEE 802.11.

WiMAX — телекомунікаційна технологія, розроблена з метою надання універсального бездротового зв'язку на великих відстанях для широкого спектру пристроїв (від робочих станцій і портативних комп'ютерів до мобільних телефонів). Заснована на стандарті IEEE 802.16, який також називають Wireless MAN.

WPA — один з протоколів безпеки, вживаних для захисту бездротових мереж. Технологія WPA передбачає шифрування даних, до того ж відбувається перевірка, чи не

було змінено мережевий ключ безпеки (цілісності). Крім того, виконується автентифікація користувачів, щоб тільки авторизовані користувачі отримували доступ до мережі.

WPA2 — стандарт IEEE 802.11i, у якому в якості основного шифру був обраний стійкий блочний шифр AES. З 2006 р. підтримка WPA2 є обов'язковою умовою для сертифікації Wi-Fi пристроїв.

Список джерел

1. *Безопасные* системы передачи конфиденциальной информации на основе протоколов квантовой криптографии : монографія / *Е.В. Василиу, В.Я. Мильчевич, С.В. Николаенко, А.В. Мильчевич.* — Х. : Цифровая типография № 1, 2013. — 168 с.

2. *Безпека* інформаційних систем і технологій : навч. пос. / *В.І. Єсін, О.О. Кузнецов, Л.С. Сорока.* — Х. : ХНУ ім. В.Н. Каразіна, 2013. — 632 с.

3. *Галицкий А.В.* Защита информации в сети – анализ технологий и синтез решений / *Галицкий А.В., Рябко С.Д., Шаньгин В.Ф.* — М. : ДМК Пресс, 2004. — 616 с.

4. *Гнатюк С.О.* Безпека інформації в інформаційно-комунікаційних системах [Текст] *: конспект лекцій / С.О. Гнатюк, М.О. Рябий* — К. : НАУ, 2013. — 131 с.

5. *Герасименко В.А.* Основы защиты информации / *В.А. Герасименко, А.А. Малюк.* — М. : МИФИ, 1997. — 537 с.

6. *Горбенко І.Д.* Захист інформації в інформаційно-телекомунікаційних системах / *І.Д. Горбенко, Т.О. Гріненко.* — Х. : 2004. — 222 с.

7. *Горбенко Ю.І.* Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика : монографія / *Ю.І. Горбенко, І.Д. Горбенко.* — Х. : Видавництво «Форт», 2010. — 608 с.

8. *Даджани Н., Кларк Д.* Средства сетевой безопасности / пер. с англ. СПб. : КУДИЦ–ПРЕСС, 2007. — 368 с.

9. *Домарев В.В.* Безопасность информационных технологий: Системный подход / *В.В. Домарев.* — К. : ООО. «ТИД ДС», 2004. — 992 с.

10. *Задірака В.К.* Методи захисту банківської інформації : підручник / *В.К. Задірака, О.С. Олексюк, М.О. Недашковський* — К. : Вища школа, 1999. — 261 с.

11. *Килин С.Я.* Квантовая криптография : Идеи и практика : монография / *С.Я. Килин, Д.Б. Хорошко, А.П. Низовцев.* — Мінськ, 2008. — 398 с.

12. *Корченко А.Г.* Построение систем защиты информации на нечетких множествах. Теория и практические решения / *Корченко А.Г.* — К. : НАУ, 2005. — 336 с.

13. *Котенко В.В.* Теория информации и защита телекоммуникации : монография / *В.В. Котенко, К.Е. Румянцев.* — Ростов-на-Дону : Изд-во «ЮФУ», 2009. — 369 с.

14. *Курітник І.П.* Безпровідна трансляція інформації / *І.П. Курітник, М.П. Карпінський.* — Тернопіль : Тайп, 2010. — 377 с.

15. *Лужецький В.А.* Інформаційна безпека : навч. пос. / *В.А. Лужецький, О.П. Войтович, А.В. Дудатьєв.* — Вінниця : Універсум-Вінниця, 2009. — 240 с.

16. *Малюк А.А.* Информационная безопасность : концептуальные и методологические основы защиты информации : учеб. пос. для вузов / *А.А. Малюк.* — М. : Горячая линия — Телеком, 2004. — 280 с.

17. *Мао В.* Современная криптография : Теория и практика / *Венбо Мао.* — М. : Издательский дом «Вильямс», 2005. — 768 с.

18. *Математичні* основи криптоаналізу : навч. пос. / *С.О. Сушко, Г.В. Кузнецов, Л.Я. Фомичова, А.В. Корабльов.* — Д. : Національний гірничий університет, 2010. — 465 с.

19. *Математичні* основи криптографії : навч. пос. / *Г.В. Кузнецов, В.В. Фомичов, С.О. Сушко, Л.Я. Фомичова.* — Д.: Національний гірничий університет, 2004. — Ч.1. — 391 с.

20. *Мохор В.В.* Наставление по кибербезопасности (ISO/IEC 27032:2012) / *В.В. Мохор, А.М. Богданов, А.С. Килевой.* — К. : ООО «Три-К», 2013. — 129 с.

21. *Нильсен М.* Квантовые вычисления и квантовая информация / *М. Нильсен, И. Чанг.* — М. : Мир, 2006. — 824 с.

22. *Новиков О.М.* Безпека інформаційно-комунікаційних систем : підручник / *О.М. Новиков, М.В. Грайворонський.* — К. : Видавництво BHV, 2009. — 608 с.

23. *Олифер В.Г.* Компьютерные сети. Принципы, технологии, протоколы. 4-е изд./ *В.Г. Олифер, Н.А. Олифер.* — СПб. : Питер, 2010. — 918 с.

24. *Панасенко С.П.* Алгоритмы шифрования. Специальный справочник. — СПб. : БХВ-Петербург, 2009 — 576 с.

25. *Романец Ю.В.* Защита информации в компьютерных системах и сетях / Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. — М. : Радио и связь, 2001. — 376 с.

26. *Румянцев К.Е.* Квантовая святи и криптография : учеб. пос. / *К.Е. Румянцев, Д.М. Голубчиков.* — Таганрог : Изд-во ТТИ ЮФУ, 2009. — 122 с.

27. *Шаньгин В.Ф.* Защита компьютерной информации. Эффективные методы и средства / *В.Ф. Шаньгин.* — М. : ДМК Пресс, 2008. — 544 с.

28. *Юдін О.К.* Захист інформації в мережах передачі даних : підручник / *О.К. Юдін, О.Г. Корченко, Г.Ф. Конахович.* — К. : Вид-во DIRECTLINE, 2009. — 714 с.

29. *Anderson R.J.* Security Engineering: A Guide to Building Dependable Distributed Systems. — Wiley Publishing Inc., 2008 — 1040 p.

30. *Computer* Security Handbook (6 edition) // *Seymour Bosworth, Michel E. Kabay, Eric Whyne.* — Wiley Publishing Inc., 2013 — 2000 p.

31. *Telecommunications* Networks: Current Status and Future Trends / *[Oleksandr Korchenko, Petro Vorobiyenko, Maksym Lutskiy, Yevhen Vasiliu, Sergiy Gnatyuk et al]* / edited by *Jesus Hamilton Ortiz.* — Rijeka, Croatia : InTech, 2012. — 446 p.

32. *Ubuntu* Hacks : Tips & Tools for Exploring, Using, and Tuning Linux // *Jonathan Oxer, Kyle Rankin, Bill Childers.* — O'Reilly Media, 2006 — 448 p.

33. *Vacca J.R.* Computer and Information Security Handbook (Morgan Kaufmann Series in Computer Security). — Morgan Kaufmann, 2009 — 928 p.

34. *Wong A., Yeung A.* Network Infrastructure Security. — Springer, 2009. — 266 p.