УДК 629.07.5

Ю.В. Стасєв, О.О. Кузнецов, Р.В. Корольов

Харківський університет Повітряних Сил імені Івана Кожедуба, Харків

АНАЛІЗ ІСНУЮЧИХ ПОСЛУГ І МЕХАНІЗМІВ ЗАХИСТУ ІНФОРМАЦІЇ

Проводиться аналіз існуючих послуг і механізмів захисту інформації відповідно до вимог міжнародних стандартів ISO/IEC 15408, ISO 7498, ISO/IEC 10181. Досліджуються перспективні напрямки розвитку криптографічних перетворень.

методи та засоби обробки інформації, захист інформації, криптографічні перетворення

Вступ

У сучасних умовах, у зв'язку з суттєвим збільшенням обсягів інформації, що обробляється на різних ланках АСУ, суттєво підвищуються вимоги до методів та засобів обробки інформації [1 – 3].

Для захисту інформації з обмеженим доступом використовуються криптографічні засоби [4 – 8]. Метою статті є аналіз існуючих послуг і механізмів захисту інформації, огляд перспективних напрямків розвитку криптографічних перетворень.

Результати аналізу

Методологічною основою розробки системи захисту інформації є стандарт ISO/IEC 15408, згідно з яким основними нормативними документами, що характеризують інформаційну систему з погляду безпеки, є профіль захисту (protection profile) і проект забезпечення безпеки (security target) [4 – 6].

Під профілем захисту розуміють незалежну множину функціональних вимог безпеки і вимог адекватності, направлених на задоволення потреб споживача. Проект безпеки є множиною вимог безпеки і специфікацій функцій безпеки.

Відповідно до основних положень міжнародних стандартів життєвий цикл системи захисту інформації складається з п'яти етапів:

1. Визначення політики безпеки, яка містить абстрактний ряд вимог до безпеки системи.

2. Аналіз вимог безпеки, включаючи аналіз ризиків, аналіз урядових, правових і стандартних вимог.

3. Визначення послуг безпеки необхідних, для задоволення поставлених вимог.

4. Побудова і впровадження системи безпеки, включаючи вибір механізмів безпеки, що забезпечують конкретні вибрані послуги безпеки.

5. Безперервне управління безпекою.

Послуга безпеки призначена для забезпечення захисту від ідентифікованої загрози і є абстрактним поняттям, яке може бути використане для характеристик вимог безпеки. Механізм безпеки є засіб, за допомогою якого реалізується і застосовується відповідна послуга. Стандарти ISO 7498, ISO/IEC 10181 визначають п'ять базових загальноприйнятих послуг безпеки: [7, 8].

– аутентифікація (authentication);

– управління доступом (access control);

– конфіденційність даних (data confidentiality);

– цілісність даних (data integrity);

– невідмова (причетність) (non-repudiation).

Додатково в ISO/IEC 10181-7 розглядається перевірка безпеки (security audit) [8].

Розглянемо базові послуги, наведені на рис. 1.

Стандарт визначає два типи послуг аутентифікації:

– аутентифікацію об'єкта;

– аутентифікацію джерела даних.

Послуга аутентифікації об'єкта необхідна в системах зі встановленням з'єднань і може застосову-

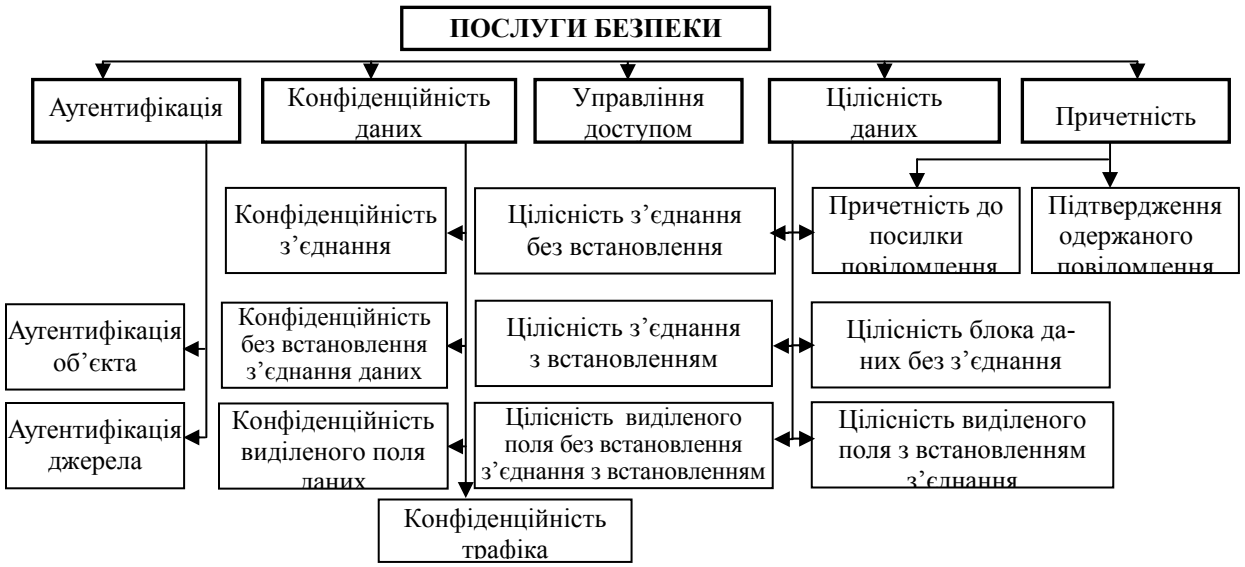

Рис. 1. Загальна класифікація послуг безпеки

ватися періодично під час сеансу. Вона служить для запобігання таким погрозам, як маскування і повтор попереднього сеансу зв'язку.

Послуга аутентифікації джерела необхідна в системах без встановлення з'єднання, для яких кожен пакет є незалежним від інших, і єдине, що може бути гарантовано з погляду аутентифікації, – це те, що джерело пакета саме те, яке вказане в його заголовку. Функція не забезпечує захисту від повторної передачі або модифікації даних.

Обидва види аутентифікації визначені для мережевого, транспортного і прикладного рівнів, на яких реалізуються протоколи з відновленням і без встановлення з'єднань.

Послуга управління доступом забезпечує доступ до ресурсів тільки авторизованих користувачів (процесів), а також гарантує відповідні права доступу для авторизованих користувачів і запобігає неавторизованому доступу як внутрішніх, так і зовнішніх користувачів.

Ця послуга застосовується до різних типів доступу до ресурсів, наприклад, використання комунікаційних ресурсів, читання, запис або видалення інформаційних ресурсів, використання ресурсів обчислювальних систем з обробки даних і т.п. та використовується для встановлення політики управління/обмеження доступу.

Під конфіденційністю розуміють властивість системи, яка гарантує, що інформація не може бути доступна або розкрита для неавторизованих (не уповноважених) осіб, об'єктів або процесів. Послуги конфіденційності поділяються на чотири типи:

– конфіденційність з'єднання забезпечує конфіденційність всіх даних користувача цього з'єднання;

– конфіденційність у режимі без встановлення з'єднання забезпечує конфіденційність всіх даних користувача в окремому блоці даних;

– конфіденційність виділеного поля даних призначена для захисту окремих інформаційних полів і вимагає, щоб тільки окремі поля в пакетах були захищені. Даний тип послуги використовується як у мережах зі встановленням з'єднання, так і в мережах без встановлення з'єднання;

– конфіденційність трафіка запобігає отриманню інформації шляхом спостереження (аналізу) трафіка. Це досягається шляхом захисту інформації про джерело.Захист цілісності даних має дві базові реалізації (для мереж зі встановленням і без встановлення з'єднання), кожна з яких може застосовуватися для вибраних груп інформаційних полів. Захист цілісності даних у мережах зі встановленням з'єднання припускає "виявлення будь-якої модифікації, включення, видалення або повторної передачі даних у послідовності (пакетів) "

Стандарт визначає п'ять типів послуги цілісності даних:

– цілісність з'єднання з відновленням забезпечує цілісність даних користувача цього з'єднання і виявляє будь-яку модифікацію, вставку, видалення або повторення даних з можливим подальшим їх відновленням;

– цілісність з'єднання без відновлення аналогічна попередній послузі, але без можливості відновлення даних;

– цілісність виділеного поля в режимі зі встановленням з'єднання забезпечує цілісність виділеного поля даних у пакеті користувача, переданих через це з'єднання;

– цілісність виділеного поля в режимі без встановлення з'єднання забезпечує цілісність виділеного поля в пакеті даних;

– цілісність блока даних без з'єднання забезпечує цілісність окремого блока даних (пакету), орієнтована на виявлення тільки модифікацій і не запобігає умисному видаленню, включенню або повторній передачі пакетів.

Під причетністю розуміють здатність запобігання можливості відмови одним з реальних учасників комунікацій від факту його повної або часткової участі в передачі даних.

Визначені дві форми послуг причетності:

– причетність до посилки повідомлення (доказ джерела) надає одержувачу доказ того, що повідомлення було послано джерелом (на випадок відмови відправника від цього факту) і цілісність не порушена;

– підтвердження (доказ) отримання повідомлень надає відправнику докази того, що повідомлення було одержано одержувачем, у разі спроб останнього відмовитися від цього факту.

Доступність визначається як додаткова послуга забезпечення захищеності інформаційних систем. Механізми забезпечення доступності запобігають атакам, що мають на своїй меті зробити ресурси або послуги інформаційної системи недоступними (або зробити їх якість незадовільною) для користувача.

На рис. 2. представлено розподіл послуг безпеки по рівнями моделі ВОС. Як випливає з наведеного рисунка, велика частина послуг безпеки доводиться на верхні рівні моделі ВОС, переважно на рівень прикладного процесу.

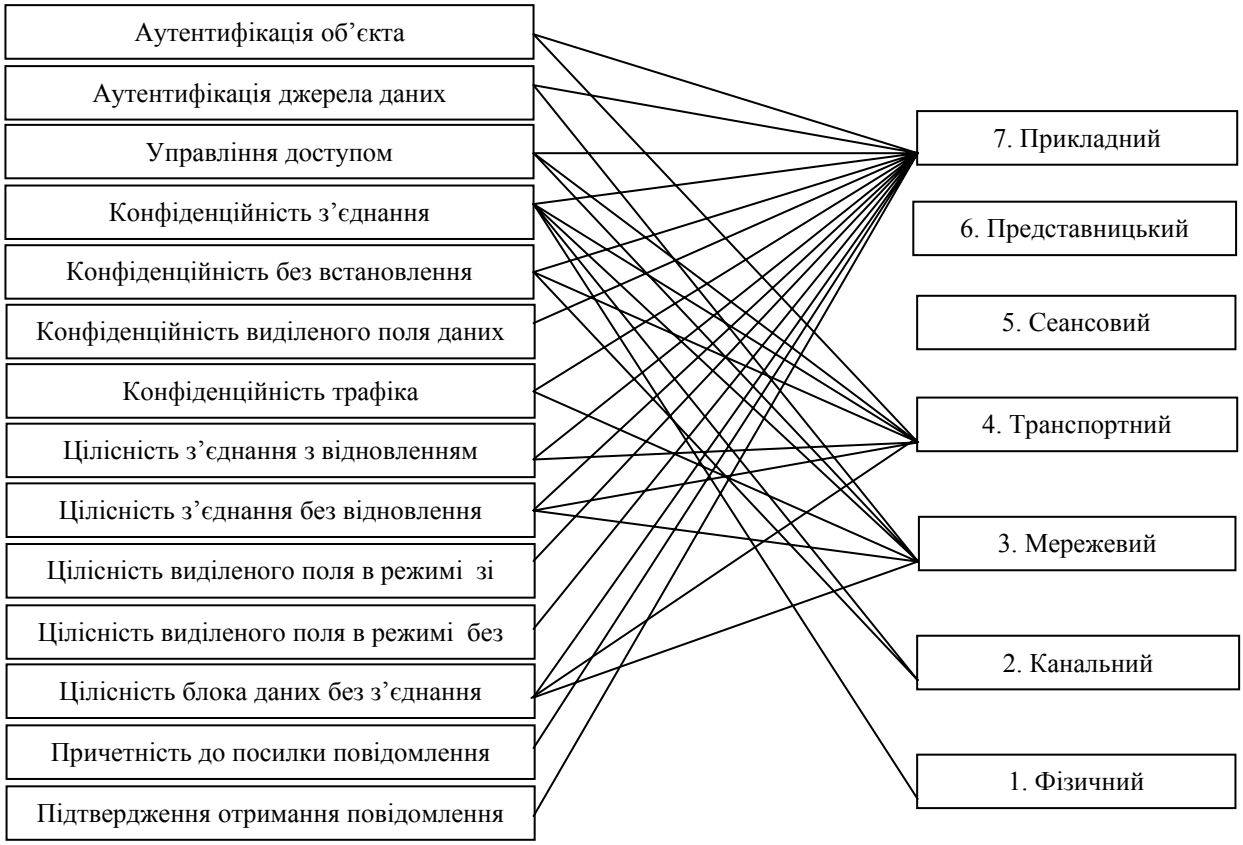

Рис. 2. Розподіл послуг безпеки за рівнями еталонної моделі ВОС

Механізми безпеки є конкретними заходами для реалізації послуг безпеки.

Стандарт ділить механізми безпеки на два класи, а саме спеціальні механізми забезпечення безпеки, які використовуються для реалізації специфічних послуг і відрізняються для різних послуг, і загальні механізми, які не відносяться до конкретних послуг безпеки (рис. 3.).

До спеціальних механізмів забезпечення безпеки відносяться такі механізми:

– шифрування (encipherment);

– механізми цифрового підпису (digital signature mechanisms);

– механізми управління доступом (access control mechanisms);

– механізми забезпечення захисту цілісності даних (data integrity mechanisms), які включають криптографічні контрольні функції;

– механізми управління доступом (access control mechanisms); механізми забезпечення захисту цілісності даних (data integrity mechanisms), які включають криптографічні контрольні функції;

– механізми аутентифікації (authentication exchange mechanisms);

– механізми заповнення трафіка (padding traffic mechanisms);

– механізми управління маршрутизацією (routing control mechanisms);

– механізми нотаризації (notarisation mechanisms).

Розглянемо кожен тип механізмів детальніше.

Механізми шифрування припускають використання криптографічних перетворень даних для того, щоб зробити їх нечитаними або неосмислювальними. Шифрування застосовується спільно із зворотною функцією – дешифруванням. Шифрування використовується для забезпечення послуги конфіденційності, але може також підтримувати інші послуги забезпечення безпеки, наприклад, аутентифікації і захисту цілісності даних.

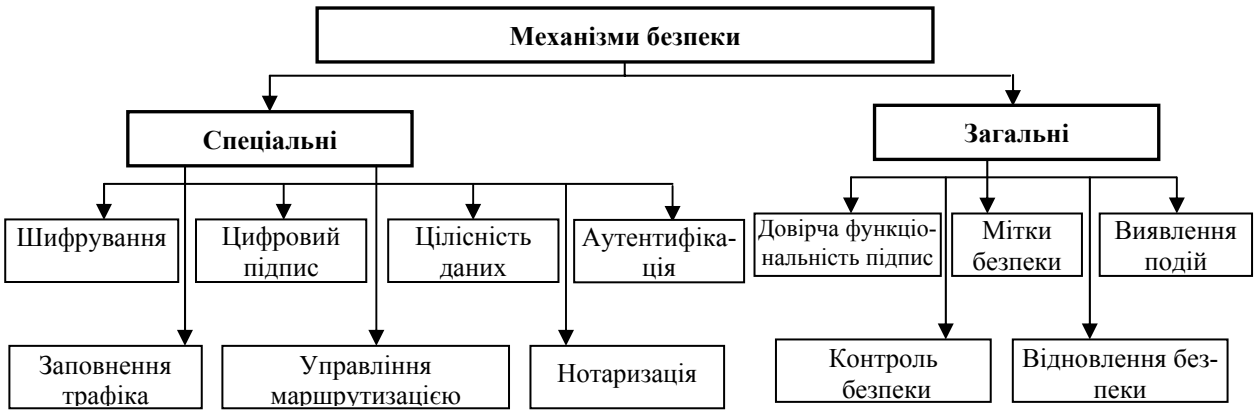

Рис. 3. Загальна класифікація механізмів безпеки

Цифровий підпис є цифровий еквівалент підпису (друк, штамп і т.п.), наявність якого в повідомленні дозволяє з високою точністю визначити джерело повідомлення (документа) і юридично довести, що з певною вірогідністю, тільки він міг створити і підписати цей документ. Механізми цифрового підпису використовують "відкриті" ключі, які генеруються відправником даних і перевіряється одержувачем. Для шифрування контрольної суми підписаного повідомлення можуть бути використані методи несиметричного шифрування. Цифровий підпис використовується для забезпечення послуг аутентифікації і захисту цілісності, для яких суб'єкт верифікації підписаних даних наперед невідомий.

Механізми управління доступом використовуються для забезпечення послуг управління доступом і реалізують політику управління доступом. При ухваленні рішень про надання запрошуваного типа доступу можуть використовуватися такі види і джерела інформації:

– бази даних управління доступом, у яких можуть знаходиться списки управління доступом або структури аналогічного призначення;

– паролі або інша ідентифікаційна інформація;

– ідентифікаційні документи або інші посвідчення, пред'явлення яких свідчить про наявність прав доступу;

– мітки безпеки, що асоціюються з суб'єктами й об'єктами доступу;

– час запрошуваного доступу;

– маршрут запрошуваного доступу;

– тривалість запрошуваного доступу й інша інформація.

Механізми цілісності даних діляться на два типи механізмів:

– механізми захисту цілісності окремого пакета даних;

– механізми захисту цілісності послідовності пакетів даних.

Цілісність окремого пакета даних забезпечується шляхом додавання до нього деякої контрольної величини, яка є функцією від даних, що містяться в пакеті. Як такі величини можуть виступати MAC-коди або криптографічні контрольні суми.

Механізми другого типу, які звичайно застосовуються спільно з механізмами захисту цілісності окремого пакета даних, можуть використовуватися для забезпечення послуг цілісності при організації зв'язку в режимі зі встановленням з'єднання. Тут використовуються такі прийоми, як нумерація пакетів, тимчасові штампи, криптографічне скріплення. Ці механізми дозволяють забезпечити захист від крадіжки, перевпорядковування, дублювання і вставки повідомлень. У мережах, що функціонують у режимі без встановлення з'єднання, використання тимчасових штампів забезпечує також і обмежену форму захисту від дублювання.

У загальному випадку під аутентифікацією розуміється встановлення достовірності повідомлення, джерела даних і приймача даних.

Аутентифікація джерела даних часто забезпечується шляхом використання механізму захисту цілісності даних спільно з шифруванням, або цифрового підпису. Логічна аутентифікація користувача комп'ютерної системи здійснюється на основі пароля. Аутентифікація об'єкта комунікації звичайно виконується за допомогою подвійного або потрійного підтвердження з'єднання або рукостискання, аналогічно процедурі синхронізації пакетів у протоколах зі встановленням з'єднання. Односторонній (одноразовий) обмін забезпечує тільки одноразову аутентифікацію і не може гарантувати своєчасність обміну. Двосторонній (двократний) обмін забезпечує взаємну аутентифікацію джерела і приймача, але не забезпечує своєчасність обміну без застосування спеціальних засобів синхронізації. Трибічний (триразовий) обмін дозволяє досягти повної взаємної аутентифікації систем без додаткової синхронізації. Тут також для забезпечення аутентифікації можуть використовуватися спеціальні механізми управління криптографічними ключами.

Механізм заповнення трафіка застосовується для забезпечення конфіденційності трафіка. Заповнення трафіка може включати генерацію випадкового трафіка, заповнення додатковою інформацією інформативних пакетів, передачу пакетів через проміжні станції в "непотрібному" напрямі. Обидва типи пакетів – як інформативний, так і випадковий, можуть

доповнюватися до постійної довжини.

Механізми заповнення трафіка ефективні тільки в поєднанні із засобами забезпечення конфіденційності, оскільки інакше зловмиснику буде очевидний фіктивний характер додаткових повідомлень.

Механізми нотаризації привертають третю сторону, що користується довірою двох суб'єктів, для забезпечення підтвердження комунікаційних характеристик даних, які передаються. Такими комунікаційними характеристиками є цілісність, час, особи відправників і одержувачів. Найчастіше механізми нотаризації застосовуються для забезпечення послуги підтвердження причетності. Для підтвердження причетності відправника даних нотаризація застосовується спільно з цифровим підписом на основі "відкритого" ключа.

Нотаризація може також застосовуватися для забезпечення надійної тимчасової мітки, що забезпечується "тимчасовим нотаріусом". Така мітка може містити підпис "нотаріуса", ідентифікатор повідомлення, імена відправника й одержувача, а також зареєстровані час і дату отримання повідомлення. При цьому "нотаріус" не має доступу до самого повідомлення, чим дотримується конфіденційність повідомлення.

Механізми управління маршрутизацією застосовуються для забезпечення конфіденційності з метою запобігання контролю за шляхом проходження даних від відправника до одержувача. Вибір шляху може здійснюватися або крайовою системою, реалізуючи маршрутизацію, визначену джерелом (sourse routing), або проміжною системою на основі використання "міток безпеки", що вводяться в пакет крайовою системою. Цей механізм вимагає забезпечення надійності (довірчості) проміжних систем і може мати істотні варіації при використанні різних систем. Він може також використовуватися і для забезпечення захисту цілісності даних (з функціями відновлення даних або з'єднання) за рахунок введення та використання для передачі даних альтернативних шляхів у разі виникнення атак, що приводять до переривання комунікацій.

До загальних механізмів забезпечення безпеки відносяться:

– довірча функціональність (trusted functionality);

– мітки безпеки (security lables);

– виявлення подій (event detection)

– контроль безпеки (security audit trail);

– відновлення безпеки (security recovery).

Довірча функціональність використовується разом з іншими механізмами безпеки і є сукупністю рекомендацій та способів, які повинні бути реалізовані для забезпечення гарантії правильної і надійної роботи інших механізмів безпеки. Довірча функціональність припускає широке використання нормативної документації при розробці програмних або апаратних засобів, що реалізують механізми безпеки. Розробка цих засобів повинна вестися при дотриманні відповідних організаційних вимог. Програмні й апаратні засоби повинні розроблятися, тестуватися і сертифікуватися на основі єдиних методик. Тут же забезпечуються всі необхідні вимоги і рекомендації до електромагнітних випромінювань, можливостей фізичного втручання, з використання безпечних каналів розповсюдження і багато що інше.

Будь-який ресурс (записані дані, обчислювальні потужності) можуть мати асоційовані з ними мітки безпеки, які позначають їх рівень секретності. Мітки безпеки можуть бути явно або побічно зв'язані як окремими пакетами даних, так і з послідовностями пакетів. Звичайно мітки безпеки використовуються для реалізації методики управління доступом на основі встановлених правил, а також для управління маршрутизацією. Дані, що передаються, також можуть мати мітки безпеки, які передаються разом з ними безпечним чином. У цьому випадку для забезпечення захисту міток застосовуються криптографічні функції, а мітки безпеки використовуються для забезпечення контролю за цілісністю повідомлень.

Механізми виявлення подій у системах захисту інформації служать для виявлення як спроб порушення безпеки, так і для реєстрації легітимної активності користувачів. Виявлення може бути локальним або дистанційним і реалізується через тривожну сигналізацію про події (event reporting (alarm)), реєстрацію подій (event logging) і відновлювальні дії (recovery actions).

Під контролем безпеки розуміють незалежний розгляд і аналіз записів безпеки з метою перевірки достатності управління системою, для того, щоб гарантувати відповідність функціонування системи політиці безпеки і рекомендувати необхідні зміни в управлінні, політиці, процесах безпеки. Звичайно розглядають дві процедури: протоколювання і аудит.

Під протоколюванням розуміється збір і накопичення інформації про події, що відбуваються в ін-формаційній системі.

Під аудитом розуміється оперативний аналіз накопиченої інформації, що проводиться постійно або періодично.

Механізми протоколювання й аудиту служать для вирішення таких завдань:

– забезпечення підзвітності користувачів і адміністраторів, що є засобом заборони;

– забезпечення можливості відновлення послідовності подій, що дозволяє виявити слабкості в захисті інформації, виявити винуватця вторгнення, оцінити масштаби заподіяного збитку і повернутися до нормальної роботи;

– надання інформації для виявлення й аналізу проблем, через підготовку відповідних звітів і рапортів.

Механізми відновлення безпеки виконують функцію реакції системи на порушення безпеки. Такими діями можуть бути, наприклад, негайне роз'єднання або припинення роботи, відмова суб'єкту в доступі, тимчасове позбавлення суб'єкта прав, занесення суб'єкта в "чорний список" і т.п.

Таким чином, як показав проведений аналіз, вживаний на сьогодні підхід забезпечення безпеки інформаційних систем полягає у виборі і подальшому використанні набору конкретних механізмів за-

хисту (профілю захисту). Взаємозв'язок послуг і механізмів безпеки представлений на рис. 4.

Рис. 4. Взаємозв'язок послуг та механізмів безпеки

Для побудови механізмів безпеки інформації традиційно використовують криптографічні методи, загальна класифікація яких наведена на рис. 5. Це методи симетричної і несиметричної криптографії: перші ґрунтуються на простих і легко реалізованих блоках підстановок і перестановок, а другі – на використанні відповідної теоретико-складної проблеми (факторизації, дискретного логарифмування та ін.).

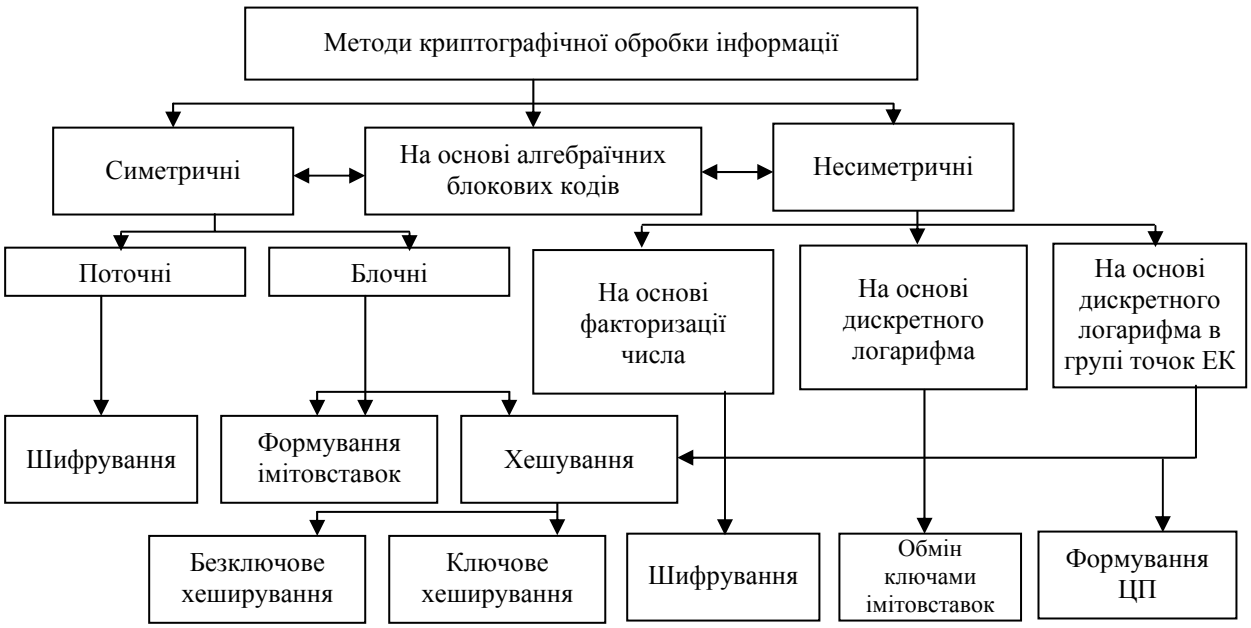

Рис. 5. Криптографічні методи захисту інформації

Одним з перспективних напрямів у розвитку сучасної криптографії є несиметричні криптосистеми, у яких, для передачі ключової інформації, не потрібна організація закритого каналу зв'язку (каналу фельд'є-

герської пошти). Застосування несиметричних криптографічних методів дозволяє звільнитися від дорогої розсилки секретних ключових даних і використовувати для обміну ключовою інформацією відкриті (загальнодоступні) канали розповсюдження. Серед відомих прикладів несиметричних криптосистем особливе місце займають секретні системи доказової стійкості, побудовані з використанням алгебраїчних кодів [9 –14]. У вітчизняній літературі вони одержали назву теоретико-кодових схем [11, 12].

Несиметричні криптосистеми на алгебраїчних кодах мають істотну перевагу – високу швидкість криптографічного перетворення інформації [11 – 14]. Крім того, як показано в [13 – 14, застосування теоретико-кодових схем дозволяє сумістити завадостійке кодування з маскуванням даних, які передаються, під випадкову послідовність і, таким чином, інтегровано (одним прийомом) підвищити достовірність та інформаційну скритність передачі даних в АСУВ.

Висновки

Таким чином, як показав проведений аналіз, перспективним напрямом інтегрованого рішення задач та забезпечення необхідних показників достовірності і інформаційної скритності (криптографічної стійкості) є застосування теоретико-кодових схем, побудованих з використанням алгебраїчних блокових кодів.

Список літератури

1. Горбенко И.Д., Потий А.В., Терещенко П.И. Рекомендации международных стандартов по оценке безопасности информационных технологий // Материалы 3 межд. НПК "Безопасность информации в информационно-телекоммуникационных системах". – К., 2000. – С. 150-160.

2. Бондаренко М.Ф., Черных С.П., Горбенко И.Д., Замула А.А., Ткач А.А. Методологические основы концепции и политики безопасности информационных технологий // Радиотехника: Всеукраинский межвед. научн.-техн. сб., 2001. – Вып. 119. – С. 5-17.

3. Горбенко И.Д., Потий А.В., Терещенко П.И. Критерии и методология оценки безопасности информационных технологий // Радиотехника: Всеукраинский межвед. научн.-техн. сб., 2000. – Вып. 114. – С. 25-38.

4. ISO/IEC 15408:2000 – Information technology-Security techniques-Evaluation criteria for IT securite.-Part 1: Introduction and general model.

5. ISO/IEC 15408:2000 – Information technology – Security techniques-Evaluation criteria for IT securite. – Part 2: Security functional requirements.

6. ISO/IEC 15408:2000 – Information technology-Security techniques – Evaluation criteria for IT securite. – Part 3: Security assurance requirements.

7. ISO 7498-2:1989 – Information technology – Open System Interconnection – Basic reference model – Part 2: Security architecture.

8. ISO/IEC 10181-(1-7):1996 – Inf. technology- Open System Interconnection – Security framework for open systems.

9. Niederreiter H. Knapsack-Type Cryptosystems and Algebraic Coding Theory // Probl. Control and Inform. Theory. – 1986. – V. 15. – P. 19-34.

11. Rao T.R.N., Nam K H. Private-key algebraic-coded cryptosystem // Cryptology. – CRYPTO 86, New York. – NY: Springer. – P. 35-48.

12. Сидельников В.М. Криптография и теория кодирования. Материалы конференции «Московский университет и развитие криптографии в России». – М.: МГУ, 2002. – 22 с.

13. Сидельников В.М., Шестаков С.О. О системе шифрования, построенной на основе обобщенных кодов Рида-Соломона // Дискретная математика. – 1992. – Т. 4, № 3. – С. 57-63.

14. Северинов А.В., Халимов Г.З. Разработка алгоритмов декодирования укороченных кодов Гоппы для каналов с ошибками и стираниями // ІКСЗТ. – Х.: ХарДАЗТ, 1998. – № 2. – С. 30-33.

15. Кузнецов А.А., Евсеев С.П. Разработка теоретико-кодовых схем с использованием эллиптических кодов // Системи обробки інформації. – Х.: ХВУ, 2004. – Вип. 5. – С. 127-132.

Надійшла до редколегії 17.10.2006

Рецензент: д-р техн. наук, проф. І.Д. Горбенко, Харківський національний університет радіоелектроніки, Харків.