УДК 681.3.06

Ю.М. ЛЄНШИНА, канд. техн. наук, А.В. ЛЄНШИН, канд. техн. наук

КРИПТОГРАФІЧНА ПІДТРИМКА ПОСЛУГ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Вступ

Несанкціонованим доступом (НСД) до інформаційних ресурсів називається, доступ здійснений з порушенням встановлених політикою безпеки правил доступу користувачів та процесів до пасивних об'єктів. Отже завданням діяльності із захисту від НСД є забезпечення дотримання правил доступу, що встановлені політикою безпекою. У цьому випадку, під політикою безпекою розуміють сукупність правил, які поділяють стани системи, у якій впроваджуються механізми захисту, на підмножини «дозволені стани» та «недозволені стани».

Захист інформації від НСД полягає в створенні і підтримці в дієздатному стані системи заходів та засобів захисту інформації, як технічних (інженерних, програмно-апаратних), так і нетехнічних (правових, організаційних), що запобігають або ускладнюють реалізацію загроз, знижують очікувані збитки. При цьому розглядаються як суб'єктивні (джерелом є людина), так і об'єктивні загрози, що є наслідками дій сил природи чи відмов обладнання [1].

Основними видами доступу, що можуть бути здійснені суб'єктами доступу (користувачами або процесами) відносно пасивних об'єктів є такі як: читання, модифікація, запуск на виконання. Керування цими видами доступу дозволяє забезпечувати такі властивості безпеки інформації, як конфіденційність, цілісність, доступність та спостереженість. Стрімкий розвиток інформаційних технологій призвів до виникнення ще однієї проблеми захисту інформації – атак, спрямованих на несанкціоноване отримання ідентифікаційних даних користувачів інформаційних систем. Для протидії зазначеним атакам на практиці реалізуються послуги приватності: анонімність, псевдонімність, прихованість та неможливість асоціації.

Незважаючи на різноманітність підходів до побудови систем захисту найчастіше використовується підхід, що передбачає забезпечення достатнього рівня захисту за мінімальних затрат на впровадження та супровід комплексної системи захисту інформації. Таким чином, актуальним є питання кількісної, або принаймні, якісної оцінки стійкості послуг захисту від НСД, що забезпечується комплексом засобів захисту (КЗЗ).

У статті досліджуються підходи, які за рахунок застосування методів криптографічної підтримки, дозволяють протидіяти загрозам несанкціонованого доступу, зокрема, загрозам порушення приватності.

Аналіз вимог національних нормативних документів в сфері захисту від НСД

У 1999 році в Україні введено в дію перші документи з серії нормативних документів з технічного захисту інформації, що визначають вимоги та порядок захисту інформації від НСД, відомих під назвою НД ТЗІ [1]. Незважаючи на те, що у наступні роки 2000 – 2012 уповноваженими органами у сфері захисту інформації України (Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України та його правонаступниками) розроблені інші документи, їх скоріше слід вважати тлумаченням окремих вимог, що були встановлені у 1999 році.

Основним з НД ТЗІ, що визначає критерії оцінки захищеності комп'ютерної системи (КС) від НСД є НД ТЗІ 2.5-004-99 [1]. У вітчизняній літературі під КС розуміється сукупність програмно-апаратних засобів, яка подана для оцінки. Тобто фактично КС є аналогом об'єкта оцінки (ТОЕ – Target Of Evaluation) за ISO/IEC 15408 [2], відомого під назвою "Єдині критерії". Встановлені у НД ТЗІ 2.5-004-99 критерії дають змогу системно розв'язувати завдання проектування КЗЗ від НСД у окремих продуктах, створення комплексних систем захисту інформації, а також проведення оцінювання відповідності розроблених КС у результаті проведень незалежних оцінювань.

Сукупність вимог (шкала оцінки), що закріплена у НД ТЗІ 2.5-004-99 застосовується для оцінювання ефективності функціональних послуг безпеки і коректності їх реалізації. Вимоги закріплені у вигляді функціональних критеріїв та критеріїв гарантій.

Функціональні критерії згруповані за ознакою властивості безпеки, для якої призначено відповідні послуги. Функціональним критерієм чи послугою безпеки, називаються правила, згідно з якими функціонують механізми, що реалізують послугу.

Критерії гарантій включають вимоги до архітектури КЗЗ, середовища розробки, послідовності розробки, випробування, середовища функціонування і експлуатаційної документації. У НД ТЗІ 2.5-004-99 вводиться сім рівнів гарантій, що є ієрархічними. Ієрархія рівнів гарантій відбиває поступово зростаючу міру впевненості, що послуги, які надаються, дозволяють протистояти загрозам, а механізми, що їх реалізують – коректно реалізовані, і можуть забезпечити очікуваний споживачем рівень захищеності інформації під час експлуатації КС.

Як випливає із аналізу змісту послуг безпеки, задача забезпечення послуги приватності у системі НД ТЗІ не розглядається. Такий стан скоріше за все зумовлений тим, що зазначена серія НД ТЗІ грунтується на принципах та правилах визначених у документах, зокрема Канадських критеріях (1993) [3], що були розроблені ще до того як проблема забезпечення приватності набула актуальності. Таким чином, можна стверджувати, що вітчизняна нормативна база на сьогодні не надає критеріїв проектування та оцінювання рішень, що забезпечують захист від загроз порушення приватності.

Аналіз вимог міжнародного стандарту ISO/IEC 15408

Міжнародний стандарт ISO/IEC 15408 відомий також під назвою "Єдині критерії" визначає вимоги до проектування, оцінювання функцій безпеки та рівнів гарантій, що реалізуються КЗЗ. ISO/IEC 15408, як і НД ТЗІ, був розроблений на основі "Канадських критеріїв" та "Федеральних критеріїв США".

Структурно ISO/IEC 15408 [2] складається з трьох частин, що визначають відповідно: базові вимоги до проектування оцінювання функцій захисту, реалізованих у ІТ-продуктах, каталог функціональних вимог безпеки та каталог вимог довіри (гарантій). З метою систематизації вимог стандарту, усі вимоги безпеки та гарантій стандарту згруповані за ієрархічним принципом: клас-родина-компонент-елемент. Класи визначають найбільш загальне групування вимог. Родини у межах класу розрізняються за ступенем суворості та іншим характеристикам вимог. Компонент є тим мінімальним набором вимог, що може бути включений до завдання з безпеки (аналог технічного завдання на КЗЗ) або профілю захисту (аналог технічного завдання на "типовий" КЗЗ). У якості елементу виступає неподільна вимога.

Між компонентами визначені залежності. Залежності виникають у випадках, коли компонент не є самодостатнім, і отже при застосуваннях компоненту, що залежить від інших, усі залежності мають бути задоволені шлях включення до технічного завдання усіх залежних компонентів.

Слід зауважити, що хоча вимоги ISO/IEC 15408 та НД ТЗІ згруповані за ієрархічним принципом, але ознаки для класифікації в них використовуються різні, з цього випливає, що послуга безпеки як основний елемент НД ТЗІ, складається з кількох компонентів ISO/IEC 15408 [2]. Класами вимог безпеки, що визначені у ISO/IEC 15408 є: аудит безпеки (FAU), зв'язок (FCO), криптографічна підтримка (FCS), захист даних користувача (FDP), ідентифікація та автентифікація (FIA), керування безпекою (FMT), приватність (FPR), захист функцій безпеки об'єкту оцінювання (FPT), використання ресурсів (FRU), доступ до об'єкту оцінювання (FTA), довірений маршрут/канал (FTP).

Проведений порівняльний аналіз змісту вимог безпеки з ISO/IEC 15408 та НД ТЗІ дозволяє стверджувати, що вони близькі за своїм наповненням, хоча ISO/IEC 15408 надає більшу гнучкість при виборі функцій безпеки, а в НД ТЗІ, нажаль, відсутні вимоги, що викликають підвищений інтерес з огляду на тему дослідження, а саме це питання: крипто-

графічної підтримки (клас FCS) та надання послуг з приватності (клас FPR).

Починаючи з першої редакції ISO/IEC 15408 [2] у ньому визначаються вимоги із забезпечення приватності. Основною задачею забезпечення приватності є: захист від розкриття ідентифікаційних даних користувача та зловживання ним з боку інших користувачів.

З метою кращого розуміння сутності вимог із забезпечення приватності у ході дослідження побудовано інформаційно-понятійну модель (рис. 1).

За результатами аналізу змісту вимог із забезпечення приватності, структури НД ТЗІ та ISO/IEC 15408 у роботі були сформульовані пропозиції з розширення функціональних послуг безпеки, що визначаються у НД ТЗІ, за рахунок критеріїв приватності. Беручи до уваги систему позначень, прийняту у НД ТЗІ, було вирішено застосовувати такі скорочення для функціональних послуг безпеки: "FPR_ANO" – "ПА", "FPR_PSE" – "ПП", "FPR_UNL" – "ПН", "FPR_UNO" – "ПР", у якості розділювача між скороченням для послуги та її рівнем за аналогією до НД ТЗІ було використано знак дефіса "-".

У табл. 1 – 3 наведені рекомендовані форми специфікації послуг "Анонімність" та "Псевдонімність", "Неможливість асоціації".

Таблиця 1

ПА-1 Анонімність	ПА-2 Анонімність без запиту інформації
КЗЗ має забезпечити, щоб [призначення: користувачі та/або суб'єкти] були не здатні визначити справжнє ім'я користувача, що пов'язаний з [призначення: суб'єкти та/або операції, та/або об'єкти]	
—	КЗЗ має надавати [призначення: послуги] для [призначення: суб'єкти] без запиту будь-якого посилання на справжнє ім'я користувача
НЕОБХІДНІ УМОВИ: НЕМАЄ	

Таблиця 2

ПП-1 Псевдонімність	ПП-2 Реверсивна псевдонімність	ПП-3 Альтернативна псевдонімність
КЗЗ має забезпечити, щоб [призначення: користувачі або суб'єкти] були не здатні визначити справжнє ім'я користувача, що пов'язаний з [призначення: суб'єкти та/або операції, та/або об'єкти]		
КЗЗ має бути здатний надати [призначення: кількість псевдонімів] псевдонімів справжнього імені користувач для [призначення: перелік суб'єктів]		
КЗЗ має бути здатний [вибір (обрати одне з): визначити псевдонім користувача, прийняти псевдонім від користувача] та перевірити його на відповідність [призначення: метрика псевдонімів]		
—	КЗЗ має надати [вибір: вповноважений користувач, [призначення: довірені суб'єкти]] можливість визначати ідентифікаційні дані користувача за наданим псевдонімом тільки за умови [призначення: умови]	КЗЗ має надати псевдонім для справжнього імені користувача, який має бути ідентичний псевдоніму наданому раніше за наступних умов [призначення: умови]; інакше наданий псевдонім має бути не пов'язаний з наданими раніше псевдонімами
—	НЕОБХІДНІ УМОВИ: НИ-1	—

Таблиця 3

ПН-1 Неможливість асоціації
КЗЗ має забезпечити, щоб [призначення: користувачів та/або суб'єкти] були не здатні визначити, що [призначення: перелік операції] [вибір: були ініційовані одним і тим самим користувачем, пов'язані наступним чином [призначення: перелік співвідношень]]
НЕОБХІДНІ УМОВИ: НЕМАЄ

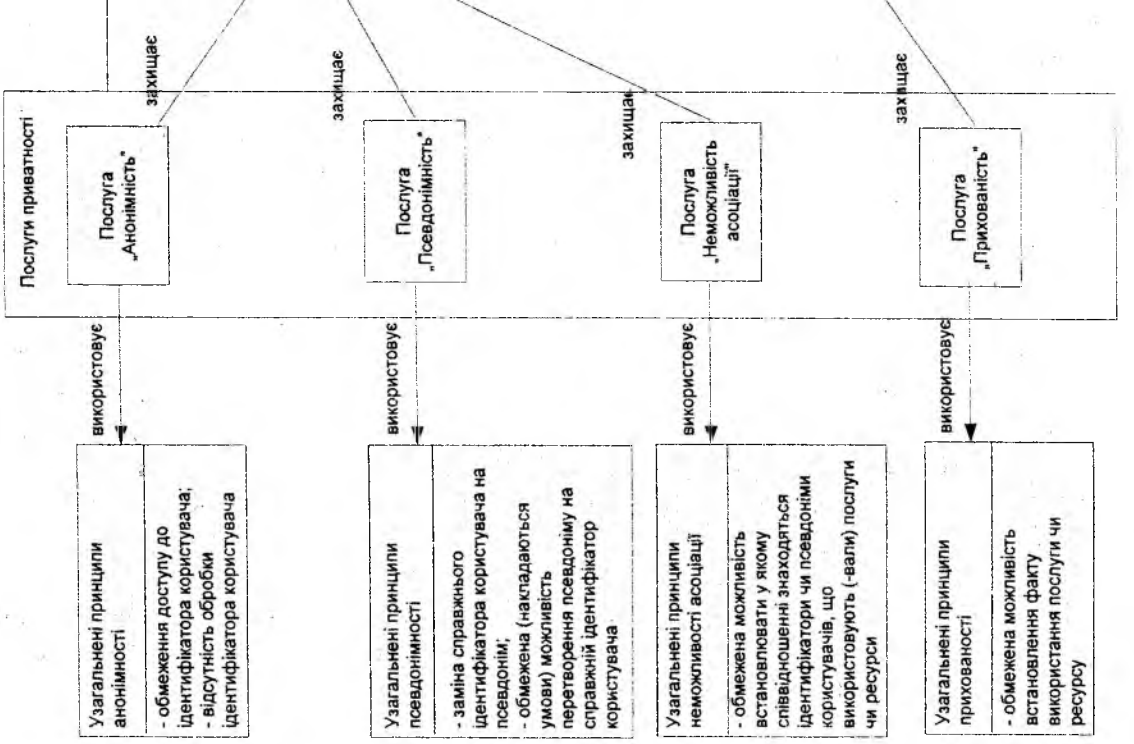
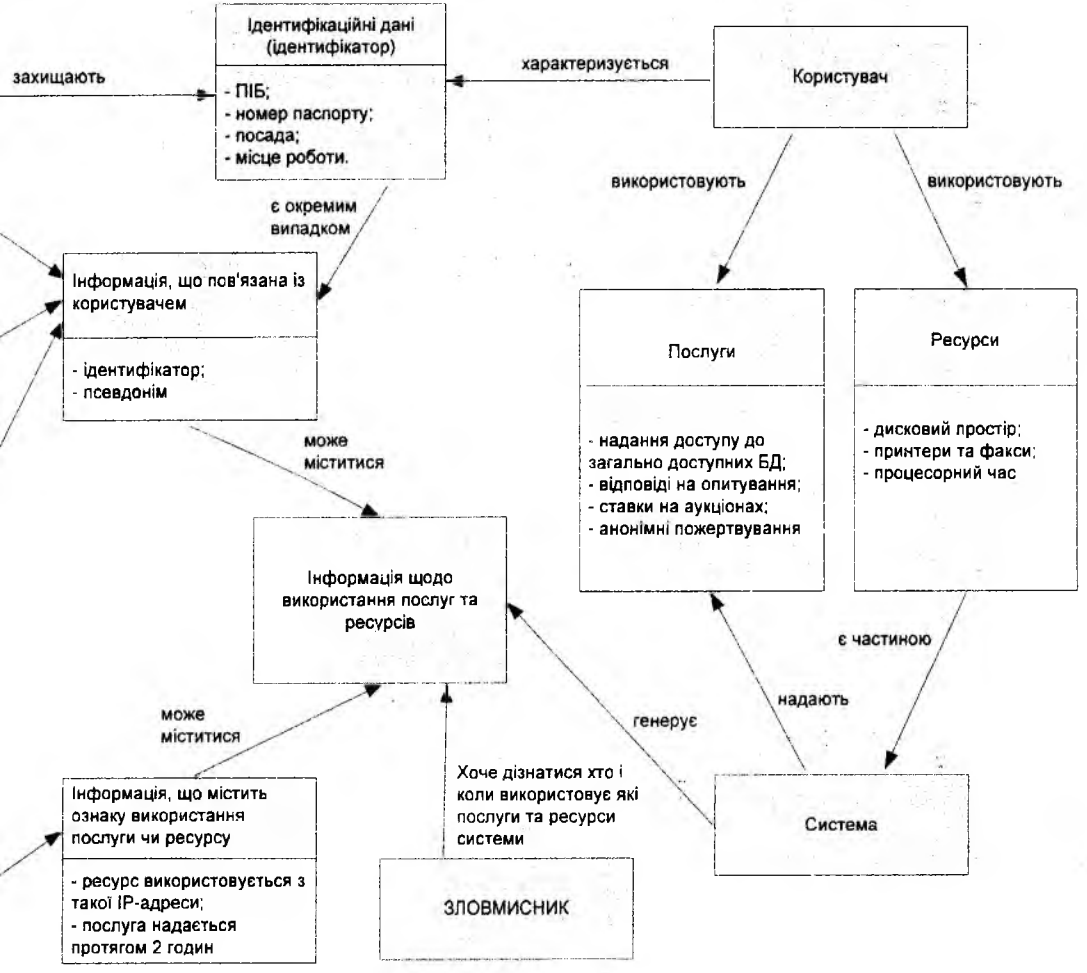

Послуги приватності
Послуга „Анонімність"
Послуга „Псевдонімність"
Послуга „Неможливість асоціації"
Послуга „Прихованість"
захищає
захищає
захищає
захищає
використовує
використовує
використовує
використовує
Узагальнені принципи анонімності
- обмеження доступу до ідентифікатора користувача;
- відсутність обробки ідентифікатора користувача
Узагальнені принципи псевдонімності
- заміна справжнього ідентифікатора користувача на псевдонім;
- обмежена (накладаються умови) можливість перетворення псевдоніму на справжній ідентифікатор користувача
Узагальнені принципи неможливості асоціації
- обмежена можливість встановлювати у якому співвідношенні знаходяться ідентифікатори чи псевдоніми користувачів, що використовують (-вали) послуги чи ресурси
Узагальнені принципи прихованості
- обмежена можливість встановлення факту використання послуги чи ресурсу

Рис.1


Ідентифікаційні дані (ідентифікатор)
- ПІБ;
- номер паспорту;
- посада;
- місце роботи.
захищають
характеризується
Користувач
використовують
використовують
є окремим випадком
Інформація, що пов'язана із користувачем
- ідентифікатор;
- псевдонім
Послуги
- надання доступу до загально доступних БД;
- відповіді на опитування;
- ставки на аукціонах;
- анонімні пожертвування
Ресурси
- дисковий простір;
- принтери та факси;
- процесорний час
може міститися
Інформація щодо використання послуг та ресурсів
є частиною
надають
може міститися
генерує
Інформація, що містить ознаку використання послуги чи ресурсу
- ресурс використовується з такої IP-адреси;
- послуга надається протягом 2 годин
Хоче дізнатися хто і коли використовує які послуги та ресурси системи
Система
ЗЛОВМИСНИК

Криптографічна підтримка та оцінювання стійкості послуг захисту від НСД

У ISO/IEC 15408 визначається, що КЗЗ може використовувати криптографічні функціональні можливості для сприяння досягненню деяких найбільш важливих цілей безпеки. Зауважується, що до них відносяться, але не обмежуються, такі цілі як: ідентифікація, неспростовність, довірений маршрут та канал, розподіл даних. Таким чином, ISO/IEC 15408, хоча і випереджає НД ТЗІ, у контексті визначення ролі та необхідності криптографічної підтримки функцій захисту від НСД, але визначає лише вимоги до "Керування криптографічними ключами" (родина FCS_CKM) та вимоги з "Криптографічних операцій" (родина FCS_COP). З аналізу сфери застосування ISO/IEC 15408 випливає, що він не ставить за мету оцінити специфічні якості криптографічних алгоритмів і, отже, не містить у своєму складі відповідних критеріїв. Передбачається, що для підтвердження стійкості проводитиметься незалежна оцінка відповідних математичних властивостей.

У Канадських критеріях [3] питанню криптографічної підтримки присвячено додаток К, що визначає, яким чином криптографія може бути використана для реалізації послуг захисту від НСД. Користуючись тим, що НД ТЗІ є правонаступницею Канадських критеріїв визначимо, що надані рекомендації щодо криптографічної підтримки таких послуг як: довірча конфіденційність (КД-1, КД-2, КД-3), адміністративна конфіденційність (КА-1 та КА-2), повторне використання об'єктів (КО-1), ідентифікація та автентифікація (НИ-1, НИ-2, НИ-3), довірений канал (НК-1 та НК-2), довірча цілісність (ЦД-1, ЦД-2, ЦД-3), адміністративна цілісність (ЦА-1 та ЦА-2), розподіл обов'язків (НО-3).

Однак проведений аналіз не свідчить, що у ISO/IEC 15408 зовсім не висувається вимог до рівня стійкості послуг безпеки. Згідно ISO/IEC 15408-1 визначається, що стійкість функції (послуги) безпеки – характеристика функції безпеки, що відображає мінімальні зусилля, які необхідні для порушення політики безпеки цієї послуги, у разі здійснення атаки безпосередньо на механізми захисту, на яких вона ґрунтується.

У ISO/IEC 15408-1 визначено такі рівні стійкості як:

- базова стійкість – захист від випадкового порушення політики послуги безпеки з боку порушників із низьким потенціалом нападу;
- середня стійкість – захист від безпосереднього/навмисного порушення політики послуги безпеки з боку порушників із помірним потенціалом нападу;
- висока стійкість – захист від ретельно спланованого та організованого порушення політики послуги безпеки з боку порушників із високим потенціалом нападу.

Слід зазначити, що у серії стандартів ISO/IEC 15408 розгляд питання стійкості криптографічних алгоритмів не входить до сфери застосування, розглядаються лише імовірнісні та перестановочні методи, що не є криптографічними. З метою оцінювання рівня довіри до реалізації послуг безпеки спільним технічним комітетом ISO/IEC JTC 1, і його підкомітетом SC 27 був підготовлений стандарт ISO/IEC 18045 «Загальна методологія оцінки безпеки інформаційних технологій», що має на меті визначення засад оцінювання на рівнях довіри EAL1 – EAL4. Таким чином, для визначення стійкості послуг безпеки необхідно визначити потенціал порушника. У додатку А ISO/IEC 18045 [4] наведено методику оцінювання потенціалу порушника, що визначається на основі зусиль, що необхідні для ідентифікації та використання вразливостей. Множина факторів, що використовується при оцінюванні рівня потенціалу та відповідні оцінки зведені до табл. 4.

Із застосуванням критеріїв з табл. 4 експерт обирає значення, що характеризують здатність зловмисника ідентифікувати чи використати вразливість. Усі обрані значення додаються і на основі результуючої суми за табл. 5 визначаються рівень потенціалу зловмисника, а також необхідний рівень стійкості послуги безпеки.

Таблиця 4

Назва фактору	Діапазон	Значення для ідентифікації вразливості	Значення для використання вразливості
Час, що витрачається порушником	< 0,5 години	0	0
	< 1 доби	2	3
	< 1 місяця	3	5
	> 1 місяця	5	8
	Непрактично	*	*
Компетентність порушника	Непрофесіонал	0	0
	Професіонал	2	2
	Експерт	5	4
Знання об'єкту атаки	Відсутність інформації	0	0
	Загальнодоступна інформація	2	2
	Чутлива інформація	5	4
Час доступу до об'єкту атаки	< 0,5 години або доступ, що не може бути викрито	0	0
	< 1 доби	2	4
	< 1 місяця	3	6
	> 1 місяця	4	9
	Непрактично	*	*
Обладнання, що може використовуватися	Відсутнє	0	0
	Стандартне	1	2
	Спеціалізоване	3	4
	Розроблене на замовлення	5	6
* – Позначає, що напад неможливий у межах часових рамок, які були б прийнятні для порушника, отже будь-яке значення «*» вказує на високий рейтинг			

Таблиця 5

Діапазон значень	Послуга безпеки протистоїть порушнику з потенціалом нападу	Рівень стійкості послуги безпеки
< 10	Рейтинг відсутній	
10 – 17	Низький	Базовий
18 – 24	Помірний	Середній
> 24	Високий	Високий

Методи і моделі криптографічної підтримки послуг захисту від НСД та рівень їх стійкості

На сьогодні не існує загальноприйнятих підходів до криптографічної підтримки послуг захисту від НСД. Проте аналіз окремих рішень та публікацій, що були використанні при вирішенні завдань захисту від НСД та їх співставлення із специфікаціями, визначених у НД ТЗІ, дозволяє описати окремі моделі та методи забезпечення криптографічної підтримки.

Модель криптографічної підтримки адміністративної конфіденційності полягає у поділі множини суб'єктів на домени та призначенні кожному з доменів власного симетричного ключа шифрування. При цьому ключ шифрування має зберігатися тільки у КЗЗ, оскільки надання ключа шифрування користувачу дозволить останньому керувати потоками інформації. Такий підхід дозволяє вирішити задачу розмежування доступу користувачів до інформації, критичної з точки зору конфіденційності, як під час збереження, так і під час експорту за межі домену, що контролюється КЗЗ, за рахунок керування ключами шифрування.

Модель, що запропонована для реалізації послуги адміністративної конфіденційності, не може бути у явному вигляді застосована для криптографічної підтримки послуги довірчої конфіденційності. Найбільш доречним тут є використання методів асиметричної криптографії, які дозволять захищати за рахунок криптографічних функцій цілісність атрибутів доступу до об'єктів захисту. Зазначена властивість досягається за рахунок надання вповноваженому користувачу ключа створення/редагування списків контролю доступу.

Криптографічна підтримка послуг адміністративної цілісності та довірчої цілісності може забезпечуватися за рахунок криптографічного протоколу, що реалізується КЗЗ, та полягає у перевірці володіння вповноваженими користувачами атрибутами доступу – відкритим ключем з визначеної адміністратором ключової пари.

Послуга повторного використання об'єктів може бути підсилена за рахунок криптографічного протоколу шифрування вмісту спільно використовуваних об'єктів. Таке шифрування не дозволить не вповноваженим суб'єктам отримати доступ до звільнених іншим процесом/користувачем пасивних об'єктів.

Модель забезпечення послуги розподілу обов'язків припускає, що функції користувачів, які притаманні певним ролям, можуть бути активовані у разі надсилання керуючих команд, що мають бути перетворені із використанням особистого ключа, що є атрибутом ролі.

Згідно із специфікацією послуги достовірного каналу, КЗЗ має забезпечувати захист від несанкціонованої модифікації та ознайомлення з атрибутами доступу користувачів, що передаються на етапах автентифікації. Зазначена задача має вирішуватися за рахунок використання криптографічних протоколів шифрування та ЕЦП.

Криптографічні протоколи, що є функціями криптографічної підтримки послуг захищеного обміну даними (конфіденційність та цілісність при обміні), ідентифікації та автентифікації, а також неспростовності відправника і одержувача, є добре дослідженими і викладені у ряді міжнародних та національних стандартів [5, 6].

Модель криптографічної підтримки послуги контролю цілісності КЗЗ передбачає наявність у КЗЗ симетричних ключів (підтримання окремого домену), а також асиметричних ключів, що можуть бути використані для контролю цілісності власних складових, наприклад за рахунок застосування механізму електронного цифрового підпису.

Слід зазначити, що незважаючи на те, що криптографічні примітиви, які використовуються як функції криптографічної підтримки, мають складність яку можна оцінити кількісно, у рамках розглянутих моделей не може бути забезпечено доказового рівня стійкості послуг захисту від НСД. Насамперед, це пов'язано з обробкою у системі таємного компоненту, який може стати відомий за рахунок неправильної реалізації, спостереженням за побічними каналами, чи внаслідок організаційних помилок. І отже стійкість цих послуг безпеки може бути оцінено лише кількісно за методикою аналогічною до викладеної у додатку А ISO/IEC 18045.

Пропонується звести задачу з подолання механізмів захисту до стійкості функцій криптографічної підтримки послуг безпеки. Відмітимо, що такий підхід не суперечить поглядам закріпленим у серії стандартів ISO/IEC 15408 [2], оскільки відповідальність за оцінку стійкості використовуваних криптографічних функцій буде віднесено до сфери відповідальності органів сертифікації у сфері КЗІ. У роботі [7] запропоновано підхід до забезпечення доказового рівня стійкості послуг захисту від НСД.

Визначення 1. Функцією криптографічної підтримки послуги захисту від НСД називають деяку функцію, яка за рахунок використання методів КЗІ, ускладнює задачу зловмисника з подолання механізмів захисту, що реалізують послугу.

Визначення 2. Захищеним станом (SEC) називається стан, у якому із заданою імовірністю у зловмисника немає доступу до інформації HI, що дозволило б йому порушити правила політики безпеки, без подолання КЗЗ.

Визначення 3. КЗЗ забезпечує доказовий рівень стійкості механізмів захисту від загроз НСД, якщо складність отримання зловмисником інформації HI не менше від припустимого значення кількісного показника.

Визначення 4. Доказовий рівень стійкості КЗЗ від загроз НСД забезпечується із застосуванням функції криптографічної підтримки, якщо HI не використовується поза її межами, а також виконується хоча б одна з таких умов:

– значення показника стійкості КЗЗ від НСД є не меншим від значення показника стійкості функції криптографічної підтримки до відомих атак (умова $\Re 1$);

– HI є закритим (таємним) параметром функції криптографічної підтримки, що не обробляється у прикладній системі (умова $\Re 2$).

Слід зазначити, що у разі забезпечення доказового рівня стійкості, атака на КЗЗ не може бути здійснена за рахунок його помилкової (хибної) реалізації чи спостереження за залишковою інформацією. Отже фактори потенціалу нападу з ISO/IEC 18045: рівень компетентності порушника, час, що витрачається, знання об'єкту атаки, час доступу до об'єкту атаки, обладнання, що використовується, буде стосуватися виключно розв'язання задачі, яка лежить в основі стійкості криптографічного перетворення, що використовується як функція криптографічної підтримки.

У роботах [8 – 9] запропоновані методи захисту від НСД в частині забезпечення захисту від загроз порушення приватності. Основою цих методів є використання у якості функцій криптографічної підтримки: групового підпису та хамелеон-підпису у групі точок еліптичної кривою. Особливістю зазначених криптопримітивів є можливість побудови моделей політики безпеки, що дозволяють на практиці виконати умову $\Re 2$ та забезпечити доказовий рівень стійкості від загроз порушення приватності.

Висновки

1. Нормативна база України не враховує світових тенденцій в напрямку забезпечення приватності користувачів інформаційно-телекомунікаційних систем. Сформульовані у роботі рекомендації щодо специфікацій послуг приватності дозволяють розширити перелік функцій захисту, що регламентується НД ТЗІ 2.5-004-99.

2. Забезпечення захисту від загроз порушення приватності є комплексною задачею, що передбачає обґрунтування вибору та впровадження послуг анонімності, псевдонімності, неможливості асоціації та прихованості. Зазначені послуги є попарно незалежними і мають обиратися згідно із розробленою для конкретної ІТС моделі загроз.

3. У НД ТЗІ 2.5-004-99 відсутні критерії стійкості послуг безпеки. Рівні стійкості послуг безпеки з ISO/IEC 15408 та методологія оцінювання з ISO/IEC 18045 дозволяють оцінити стійкість послуг безпеки лише із застосування експертних оцінок на якісному рівні.

4. Використовувані сьогодні моделі та криптографічні протоколи підтримки "базових" послуг безпеки, пов'язаних із розмежуванням доступу, передачею каналами зв'язку, ідентифікацією/автентифікацією не можуть забезпечити доказовий рівень стійкості, оскільки передбачають обробку у системі таємного компоненту, що може бути скомпрометований, наприклад за рахунок побічних каналів витоку інформації.

5. Застосування механізмів групового підпису та методів хамелеон-гешування, хамелеон-підписів дозволяє надавати криптографічну підтримку послуг приватності із доказовим рівнем стійкості.

Список літератури: 1. *НД ТЗІ* 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. 2. *ISO/IEC 15408* – 2. Information technology–Security techniques–Evaluation criteria for IT security – Part 2. Security functional requirements. 3. *Canadian* Security Establishment (CSE), "The Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)", Version 3.0, January 1993. 4. *ISO/IEC18045*. Information technology – Security techniques – Methodology for IT security evaluation. 5. *ДСТУ* ISO/IEC 13888-1:1997 "Інформаційні технології. Методи захисту. Неспростовність. Ч. 1. Загальні положення". 6. *ДСТУ* ISO/IEC 9798-3:2006 "Інформаційні технології. Методи захисту. Автентифікація об'єктів. ". Ч. 3. Механізми, що ґрунтуються на використанні алгоритмів цифрового підпису. 7. *Лєншина, Ю.М.* Модель системи обслуговування замовлень з доказовим рівнем стійкості механізмів захисту від загроз приватності та неспростовності джерела / Ю.М. Лєншина // Системи обробки інформації. – Х., 2011. – Вип. 3(19). – С. 213 – 225. 8. *Погребняк, К.А.* Анализ современных групповых подписей на основе парных отображений и перспективы их использования в национальном электронном документообороте / К.А. Погребняк, Ю.М. Іщенко // Радіоелектронні і комп'ютерні системи. – Х., 2010. – Вип. 6(47). – С. 94 – 98. 9. *Лєншина, Ю.М.* Реалізація послуги приватності у схемі інтернет-аукціону з використанням хамелеон-підпису / Ю.М. Лєншина, Д.С. Беляк // Системи обробки інформації. – Х., 2011. – Вип. 3(93). – С. 126 – 129.

Харківський національний університет радіоелектроніки

Надійшла до редколегії 23.09.2012