3 Забезпечення захисту інформації в системах зв'язку. Технічні засоби системи захисту інформації

УДК 681.321;322:621.395

РОЗПОДІЛ РЕСУРСІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ ЗАГАЛЬНОГО КОРИСТУВАННЯ

Володимир Кононович, Тетяна Тардаскіна*, Сергій Гладиш*

*Академія зв'язку України, Одеський регіональний центр ТЗІ ВАТ "Укртелеком", *Одеська національна академія зв'язку*

Анотація: **Аналізується розподіл послуг та механізмів інформаційної безпеки телекомунікаційних мереж загального користування, який рекомендується міжнародними стандартами МСЕ X.800, X.805. Розглядається метод оцінки варіанту розподілу механізмів інформаційної безпеки.**

Summary: **The division services end mechanisms of information security of the telecommunication systems (for general use) which ITU-T Recommendation X.800, X.805 analyzed. The division method assessment of mechanisms information security is considered.**

Ключові слова: **Інформаційна безпека, телекомунікаційні мережі, передавання даних, загрози, послуги та механізми безпеки.**

I Вступ

Законом України "Про телекомунікації" та низкою галузевих нормативних актів встановлені вимоги щодо забезпечення інформаційної безпеки телекомунікаційних мереж загального користування з метою створення перешкод для будь-якого несанкціонованого втручання у процес функціонування мереж, забезпечення захисту від спроб викрадення, модифікації, виведення з ладу або знищення компонентів мережі, а також забезпечення захисту від викрадення, знищення, перекручення, блокування, несанкціонованого витоку інформації та від порушення встановленого порядку її маршрутизації [1, 2]. Безпечна телекомунікаційна мережа має бути захищена проти зловмисних й ненавмисних атак, бути надійною, масштабованою, забезпечувати гарантований час відповіді, доступність послуг та інформації, цілісність інформації та обладнання та точність білінгової інформації. Захищеність складових елементів телекомунікаційної мережі є вирішальним для безпеки всієї мережі, включаючи застосування та сервіс. Але, оскільки в мережі об'єднується велика кількість елементів, то успішність рішень визначає їх здатність до взаємодії або відсутність такої здатності. Інформаційна безпека повинна забезпечуватись не лише від загроз кожному елементу або сервісу, а має бути забезпечена у взаємодії засобів і заходів безпеки в мультимедійному середовищі за повної комплексної реалізації безпеки передачі інформації з кінця в кінець. Задача розподілу ресурсів інформаційної безпеки та оцінки ефективності розподілу залишається поки що невирішеною [3 – 9, 16], але продовжує бути актуальною.

Метою даної роботи є аналіз способів розподілу послуг та механізмів інформаційної безпеки телекомунікаційних мереж загального користування, які встановлюються рекомендаціями міжнародного союзу електрозв'язку (МСЕ).

Постановка задачі. Задача вирішується шляхом порівняння положень міжнародних рекомендацій з положеннями чинної в Україні нормативно-правової бази системи технічного захисту інформації (ТЗІ). Розглядається також метод оцінки ефективності вибору варіантів побудови системи інформаційної безпеки, яка забезпечує виконання політики інформаційної безпеки телекомунікаційних мереж та прийнятний рівень інформаційної безпеки при допустимій величині витрат. Оцінка захищеності інформаційних ресурсів пов'язується з задачами моніторингу інформаційної безпеки телекомунікаційних мереж з метою одержання статистики експлуатації системи забезпечення інформаційної безпеки (СЗІБ).

Розподіл послуг безпеки за рівнями моделі архітектури взаємодії відкритих систем (ВВС) згідно з Рекомендаціями МСЕ X.200, X.800 [6, 7] проаналізовано в [3]. Деталізація розподілу механізмів безпеки подається в Рекомендаціях МСЕ X805 [8], у якій розглядається архітектурні елементи, що можуть забезпечити інформаційну безпеку для систем передачі інформації з кінця в кінець.

II Особливості архітектури та механізми забезпечення інформаційної безпеки телекомунікаційних мереж

Архітектура інформаційної безпеки визначає план та набір принципів, які описують структуру СЗІБ передачі інформації телекомунікаційною мережею з кінця в кінець. У даному випадку синонімами виразу "End-to-end communications" можуть бути поняття "з'єднання типу точка-точка", "з'єднання (зв'язок) кожного з кожним", "з'єднання з кінця в кінець". Рекомендація МСЕ X800 [7] поділяє загрози на навмисні й випадкові і описує наступні загрози інформаційним ресурсам телекомунікаційних мереж: знищення інформації і/або інших ресурсів, спотворення (псування) або модифікація інформації, розкрадання, видалення або втрата інформації і/або інших ресурсів, розкриття (компрометація) інформації, переривання послуг.

Згідно з рекомендацією МСЕ X805 [8] інформаційна безпека телекомунікаційних мереж має забезпечуватись в умовах інтеграції інформаційних та телекомунікаційних технологій, конвергенції мереж і застосовуватись до радіо, оптичних і металевих голосових ліній зв'язку та передачі даних, а також в умовах дії на мережах операторів різних форм власності. Архітектура інформаційної безпеки забезпечує всебічне, зверху-вниз та з кінця в кінець комплексну безпеку мереж та може застосовуватись до елементів, служб і застосувань для виявлення, прогнозування і коригування уразливості безпеки. Захисту підлягають усі складові елементи телекомунікаційних мереж: лінії, канали, системи передавання, обладнання, програмне забезпечення, інформація та персонал. Необхідно узгоджувати методи забезпечення інформаційної безпеки різних компонентів телекомунікаційних мереж, включаючи інформаційні ресурси, застосування, телекомунікаційні протоколи. Комплексний підхід означає необхідність створення мережної інфраструктури забезпечення інформаційної безпеки, оскільки вразливість будь-якої ланки мережі може створити проблеми для усіх її учасників – провайдерів, операторів і споживачів послуг. Кінцевою метою є вибір ефективних засобів протидії загрозам при реалізації системи інформаційної безпеки, вартість витрат на яку не перевищує вартості втрат, очікуваних від реалізації загроз.

Архітектура інформаційної безпеки логічно поділяє складний комплекс мережі між її кінцевими пунктами на окремі архітектурні компоненти інформаційної безпеки. Такий поділ враховує систематичний комплексний підхід до інформаційної безпеки з'єднання з кінця в кінець, який може використовуватись для планування засобів безпеки, а також для оцінки безпеки існуючих мереж. Архітектура інформаційної безпеки будується з врахуванням загроз, проти яких необхідний захист, особливостей типів обладнання мереж, властивості групового обладнання та типів функцій мереж, які необхідно захищати. Архітектура інформаційної безпеки розглядається у трьох архітектурних компонентах: механізмах безпеки, рівнях забезпечення безпеки та площинах забезпечення безпеки. Принципи, описані архітектурою інформаційної безпеки, можуть бути застосовані до широкого різноманіття телекомунікаційних мереж незалежно від застосованої технології або розміщення в протокольному стеку.

Механізмами забезпечення інформаційної безпеки називають набір заходів безпеки, які захищають проти всіх головних загроз безпеки, підтримують політику безпеки, яка визначена для окремої мережі, і сприяють дотриманню набору правил менеджменту безпеки. Механізми інформаційної безпеки не обмежуються мережею, а розповсюджуються на застосування, кінцевих користувачів та використовуються провайдерами служб або підприємствами, які надають послуги безпеки, маючи ліцензії на цей вид діяльності. Механізмами інформаційної безпеки є: керування доступом, автентифікація, неспростовність причетності до участі в обміні, конфіденційність даних, безпечність комунікацій (з'єднання), цілісність даних, доступність та приватність.

Механізми забезпечення контролю доступу захищають проти неавторизованого використання ресурсів мережі. Контроль доступу гарантує, що лише авторизованим суб'єктам або пристроям дозволений доступ до елементів мереж, інформації, інформаційних потоків, послуг та застосувань. Зокрема, роле-орієнтований контроль доступу забезпечує різні рівні доступу, який гарантує, що суб'єкти можуть отримати доступ і виконувати дії з елементами мереж, інформацією і потоками інформації, до яких вони уповноважені.

Механізми забезпечення автентифікації служать для підтвердження ідентичності взаємодіючих суб'єктів. Автентифікація гарантує валідність та законність об'єктів та суб'єктів, які беруть участь у взаємодії (приміром, осіб, пристроїв, служб або застосувань) і забезпечує гарантію, що суб'єкт не робить спробу маскараду (маскування під авторизованого користувача) або неправомочного повтору попереднього зв'язку.

Механізми забезпечення неспростовності участі у обміні забезпечують засоби для попередження спроби відмови суб'єкта від виконаних специфічних дій відносно даних, а також доступності доказів різних дій, зв'язаних з телекомунікаційною мережею (таких як доказ зобов'язання, намірів або вручення,

доказів авторства (джерела) даних, доказів володіння, доказів використання ресурсу). Ці механізми гарантують доступність свідчень, які можуть бути подані третьою стороною і використані для доказу, що мав місце деякий випадок або деякий наслідок події.

Механізм забезпечення конфіденційності даних захищає дані від неавторизованого розкриття. Конфіденційність даних гарантує, що зміст даних не може бути зрозумілим неавторизованому суб'єкту. Для забезпечення конфіденційності даних часто використовуються методи шифрування, списки контролю доступу і допустимих файлів.

Механізми забезпечення безпечності зв'язку гарантують, що потоки інформації протікають лише між авторизованими кінцевими пунктами, що інформація не витікає або не перехоплюється із інформаційного потоку між цими кінцевими пунктами.

Механізми забезпечення цілісності даних гарантують коректність або точність даних. Дані захищені від неправомочної модифікації, видалення, створення та копіювання даних і, крім того, забезпечується індикація цих неправомочних дій.

Механізми забезпечення доступності гарантують, що події, які впливають на мережу, не призводять до відмови від авторизованого доступу до елементів мережі, інформації, інформаційних потоків, послуг і застосувань. У цю категорію включені засоби відновлення після катастроф, аварій та відмов обладнання телекомунікаційної мережі.

Механізми забезпечення приватності (Privacy) забезпечують захист інформації, яка може бути отримана від спостереження за функціонуванням мережі. Прикладом такої інформації можуть бути WEB-сторінки, які відвідав користувач, географічне місце розташування користувача, IP-адреси або DNS-імена пристроїв в телекомунікаційній мережі провайдера послуг. У вітчизняних нормативно-правових документах сфери ТЗІ механізми забезпечення приватності не визначаються, що певно є наслідком відсутності в Україні традицій недоторканості приватної власності. Але Конституцією України, Законом України "Про телекомунікації", (стаття 9), Ліцензійними умовами [10, 11] та іншими нормативними актами закріплена норма захисту таємниці зв'язку, "забезпечення конфіденційності інформації, яка стосується споживача, забезпечення і відповідальності за схоронність відомостей щодо споживача, отриманих при укладені договору, наданих телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, їх оплати, маршрутів передавання тощо" [10]. Механізми забезпечення приватності інформації щодо споживача повинні застосовуватись навіть в тому випадку, коли договором не передбачається надавання послуги забезпечення конфіденційності інформації споживача.

Механізми забезпечення інформаційної безпеки застосовуються для протидії певній множині загроз. У табл. 1 відображається низка загроз, яким протистоять кожен з механізмів інформаційної безпеки.

Таблиця 1 – Матриця відповідності механізмів безпеки загрозам безпеки, яким вони протистоять

Механізми інформаційної безпеки	Загрози безпеці інформації та іншим ресурсам				
	Знищення	Спотворення чи модифікація	Крадіжка або втрата	Розкриття (компрометація)	Перериванн я послуг
Керування доступом	+	+	+	+	-
Автентифікація	-	-	+	+	-
Неспростовність	+	+	+	+	+
Конфіденційність	-	-	+	+	-
Безпечність з'єднання	-	-	+	+	-
Цілісність	+	+	-	-	-
Доступність	+	-	-	-	+
Приватність	-	-	-	+	-

Позначка "+", яка сформована на перетині колонок та рядків таблиці, позначає, що окремій загрозі безпеці протистоїть відповідний механізм інформаційної безпеки.

III Ієрархічна рівнева архітектура забезпечення інформаційної безпеки

Для забезпечення інформаційної безпеки телекомунікаційних мереж з кінця в кінець механізми безпеки повинні застосовуватись до ієрархії обладнання мережі з групуванням їх у сімейства засобів , які описуються як рівні забезпечення безпеки. В свою чергу, на кожному з рівнів функціонують деякі типи механізмів інформаційної безпеки, які кваліфікуються як площини інформаційної безпеки.

Визначено такі ієрархічні рівні мережно-орієнтованих засобів забезпечення інформаційної безпеки: рівень забезпечення інформаційної безпеки інфраструктури, рівень забезпечення безпеки послуг, рівень забезпечення безпеки застосувань. Рівні забезпечення інформаційної безпеки є послідовністю

взаємозалежних засобів безпеки мереж: рівень забезпечення безпеки інфраструктури взаємозалежить від рівня забезпечення безпеки послуг, а рівень забезпечення безпеки послуг взаємозалежить від рівня забезпечення безпеки застосувань. Кожен рівень має різні уразливості безпеки. Механізми інформаційної безпеки застосовуються до рівнів забезпечення безпеки, щоб зменшити вразливості, які існують на кожному рівні та, таким чином, послабити атаки на безпеку. На кожному з рівнів пропонується така гнучкість механізмів протидії потенційним загрозам, яка найбільш придатна для окремого рівня інформаційної безпеки. У Рекомендації МСЕ X.805 підкреслюється, що всі три рівні забезпечення інформаційної безпеки можуть бути застосовані до кожного з семи рівнів моделі взаємодії ВВС, оскільки кожен рівень моделі ВВС має свою інфраструктуру, надає свої послуги і має свої застосування.

Рівень забезпечення інформаційної безпеки інфраструктури телекомунікаційної мережі складається із засобів обслуговування передачі інформації мережею, а також індивідуальних елементів мережі, захищених за допомогою механізмів інформаційної безпеки. Рівень інфраструктури складається з основних блоків мереж, служб та застосувань. Прикладами компонентів, які належать до рівня інфраструктури, є індивідуальні маршрутизатори, комутатори та служби, а також канали зв'язку між індивідуальними маршрутизаторами, комутаторами та серверами.

Рівень забезпечення інформаційної безпеки послуг відноситься до інформаційної безпеки служб, які провайдери послуг забезпечують їх клієнтам. Ці послуги надаються як транспортні функції та підключення до служб, які дають забезпечення доступу до телекомунікаційної мережі або до Інтернет (наприклад сервіс автентифікації, авторизації та спостережності (AAA), сервіс динамічної конфігурації хоста, сервіс доменних імен тощо), до додаткових служб типу телефонної служби, служби якості сервісу (QoS), віртуальних приватних мереж (VPN), послугам місця розташування, термінового передавання повідомлень тощо. Рівень інформаційної безпеки послуг використовується для захисту провайдерів послуг та їх клієнтів, які є потенційними цілями загроз безпеки. Для прикладу, нападаючі можуть спробувати блокувати можливості провайдера послуг, або переривати можливість обслуговування індивідуальних клієнтів.

Рівень забезпечення інформаційної безпеки застосувань зосереджений на безпеці мережне-базованих застосувань, доступних клієнтам провайдера послуг. Ці застосування дають змогу мережним службам та центрам даних виконувати функції транспорту (передачі) файлів (FTP) і застосувань web browsing, довідкові функції управління, передачі голосових повідомлень та e-mail, а також високорівневі функції, такі як керування телекомунікаціями користувача, електронна комерція, дистанційне навчання, відео конференції тощо. На цьому рівні є такі потенційні цілі для атак на безпеку: застосування користувача, застосування провайдера та провайдер служби.

Площина інформаційної безпеки – це деякий тип механізмів інформаційної безпеки, функціонуючих у захищеній мережі. Визначаються такі площини безпеки інформації для представлення трьох типів захищеного функціонування, яке має місце у мережі: площина безпеки менеджменту, площина безпеки сигналізації та контролю, площина безпеки кінцевого користувача. Ці площини безпеки характеризують специфічні потреби інформаційної безпеки, пов'язані з виконанням менеджменту мережі, організацією контролю і сигналізації мережі, та відповідними діями кінцевого користувача. Мережі повинні проектуватись таким чином, щоб події на одній площині безпеки були б повністю ізольовані від подій у інших площинах безпеки. Наприклад, потік запитів до служби доменних імен (DNS) у площині кінцевого користувача, ініційованих запитами кінцевого користувача, не повинні блокувати інтерфейс керування, адміністрування, технічного обслуговування та забезпечення (OAM&P) у площині менеджменту, який дозволяв би адміністратору виправляти проблему. Кожен тип описаних функцій мережі має свої власні специфічні потреби безпеки. Концепція площин інформаційної безпеки дозволяє диференціювати специфіку безпеки відносно пов'язаних з ними дій і можливістю розглядати їх незалежно. Наприклад, у службі передачі голосу за допомогою IP (VoIP) послуги служби безпеки розподіляються по рівням таким чином, що захист менеджменту служби VoIP (приміром обслуговування користувачів) повинен бути незалежним від захисту служби контролю та сигналізації (наприклад, протоколу типу SIP), а також бути незалежними від захисту даних (голосу) кінцевого користувача, які транспортуються мережею.

В *площині забезпечення безпеки менеджменту* розглядається захист функцій OAM&P у елементах мережі, засобах обслуговування передачі, системі надавання базових послуг (системі підтримки функціонування, системі підтримки бізнесу, системі піклування про клієнта тощо), та центрах даних. Площина менеджменту підтримує функцій надійності, працездатності, адміністрування, постачання (забезпечення) та безпеки (FCAPS). Підмережа, яка передає трафік у інтересах менеджменту, може бути спільно канальною та зовнішньо канальною відносно трафіка користувача.

В *площині забезпечення безпеки контролю та сигналізації* розглядається захист функціонування, яке забезпечує ефективну доставку інформації, послуг та застосувань через мережу. Сюди включаються

функції керування встановленням з'єднання, які дозволяють вузлам комутації (наприклад комутаторам і маршрутизаторам) визначати найкращі маршрути для трафіка через основну транспортну мережу. Цей тип інформації називають контрольною або сигнальною інформацією. Підмережа, яка передає контрольно-сигнальну інформацію також може бути спільно канальною або зовнішньо канальною відносно трафіка користувача. Для прикладу, IP мережі несуть керуючу інформацію в пакетах, тобто всередині каналу, тоді як у комутованих телефонних мережах загального користування (PSTN) керуюча інформація передається у окремих (зовнішньо канальних) системах сигналізації (SS7). Трафік такого типу включають протоколи маршрутизації DNS, SIP, SS7, Megaco/H.248, H.242 тощо.

Площина забезпечення безпеки кінцевого користувача направлена на забезпечення безпеки доступу та безпеки використання мережі провайдера послуг клієнтами. Ця площина також описує дійсні потоки даних кінцевого користувача. Кінцевий користувач може використовувати мережу, яка забезпечує тільки з'єднання (комутацію), або використовувати додатково служби типу VPNs, або може використовувати доступ до мережне-базованих застосувань.

Рис. 1 ілюструє архітектуру інформаційної безпеки у телекомунікаційних мережах загального користування. Рисунок зображає концепцію захисту мережі механізмами захисту в кожній площині інформаційної безпеки з кожним рівнем забезпечення інформаційної безпеки, щоб протидіяти визначеним загрозам безпеці та щоб зменшити вразливості, які існують на кожному рівні та площині і, таким чином, послабити атаки на безпеку.

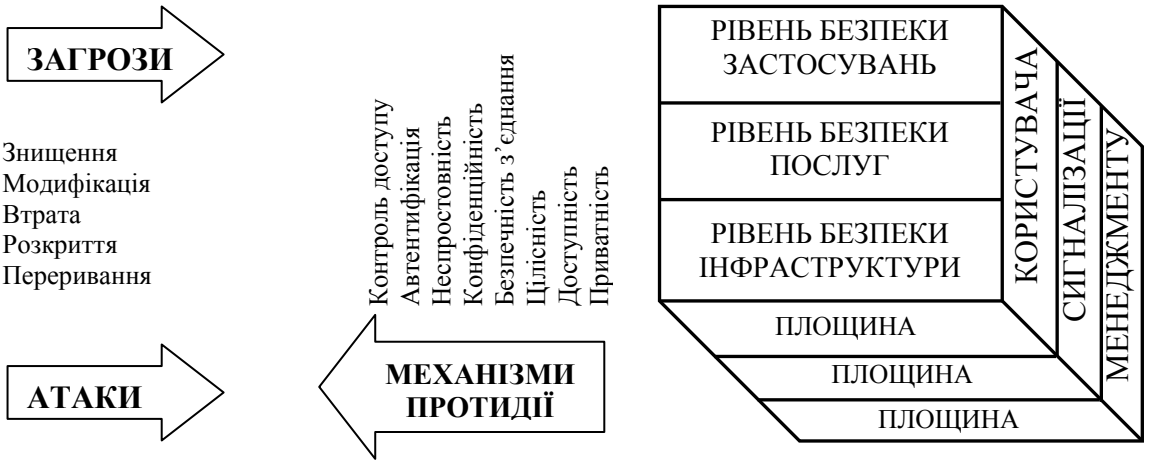

Рисунок 1 – Архітектура інформаційної безпеки телекомунікаційної мережі передачі інформації з кінця в кінець

Методичний підхід до інформаційної безпеки телекомунікаційної мережі полягає у розгляді кожного механізму безпеки на кожному рівні забезпечення інформаційної безпеки та кожній площині інформаційної безпеки. Утворюється дев'ять модулів безпеки, кожен з яких комбінує вісім механізмів безпеки, які застосовуються до окремого рівня забезпечення безпеки в окремій площині інформаційної безпеки. При цьому ясно, що залежно від вимог до даної мережі, можливо не потрібно мати всі запроваджені архітектурні елементи, тобто інколи не потрібно мати повний набір механізмів безпеки, рівнів забезпечення інформаційної безпеки або площин забезпечення інформаційної безпеки.

Архітектура інформаційної безпеки може застосовуватись до всіх аспектів і стадій забезпечення програми інформаційної безпеки. Програма забезпечення інформаційної безпеки складається з політики і процедур в додаток до технології. Вона проходить через такі стадії протягом життєвого циклу СЗІБ: технічного завдання, проектування, експлуатації. Архітектура безпеки може застосовуватись при визначенні політики інформаційної безпеки та процедур, а також технологій по всім фазам програми безпеки та життєвого циклу. Архітектура безпеки може сприяти розвитку загальної політики безпеки, реагування на інциденти та плани відновлення, архітектури технології протягом стадій технічного завдання та проектування. Архітектура безпеки може також бути використана як основа для оцінки інформаційної безпеки. В продовж стадії експлуатації мереж реалізована програма забезпечення інформаційної безпеки повинна підтримувати поточну інформаційну безпеку при змінах навколишнього середовища. Архітектура інформаційної безпеки може допомагати в керуванні політикою та процедурами безпеки, в реагуванні на інциденти та в планах відновлення системи інформаційної безпеки.

Архітектура інформаційної безпеки також може застосовуватись до будь-якої мережі на будь-якому рівні протокольного стеку. Наприклад, в IP-мережі, яка реалізується на трьох рівнях протокольного стеку, рівень інфраструктури описує індивідуальні маршрутизатори, канали зв'язку типу точка-точка між маршрутизаторами і серверні платформи для забезпечення підтримки служб, необхідних у IP-мережі. Рівень послуг відноситься до основної служби безпосередньо (таких як здатність підключення до Internet), IP підтримує служби (такі як, AAA, DNS тощо), та просунуті додаткові служби, які пропонує провайдер послуг (такі як VoIP, QoS, VPN, тощо). Нарешті, рівень застосувань описує безпеку застосувань користувача, до яких надається доступ через IP-мережу типу e-mail.

Аналогічно, для мережі з асинхронним методом переносу (ATM), яка позиційована на двох рівнях протокольного стеку, рівень інфраструктури описує індивідуальні комутатори та канали зв'язку типу точка-точка між комутаторами. Рівень послуг описує різні класи пропонованих засобів транспорту (постійної швидкості передавання, змінної швидкості передавання у режимі реального часу, змінної швидкості передавання не у режимі реального часу, доступну швидкість передавання і не специфіковану швидкість передавання). Нарешті, рівень застосувань стосується використання кінцевим користувачем мережі ATM для доступу до застосування типу відео конференцій.

IV Завдання, які досягаються застосуванням механізмів інформаційної безпеки

Механізми інформаційної безпеки різних модулів безпеки мають різні завдання і, як наслідок, містять в собі різні набори заходів безпеки. У Рекомендації МСЕ X.805 деталізовані комбінації механізмів інформаційної безпеки по кожному з дев'яти модулів безпеки. У цій роботі розглянемо найбільш цікаві, з нашого погляду, варіанти застосування механізмів безпеки на рівні безпеки застосувань у площині безпеки кінцевого користувача та застосування механізму приватності в усіх дев'яти модулях безпеки.

Забезпечення безпеки в площині кінцевого користувача прикладних рівнів полягає в забезпеченні безпеки даних користувача в мережне-базованих застосуваннях. Для прикладу, конфіденційність номерів кредитних карток користувачів повинна бути захищена в застосуваннях е-комерції. На рівні застосувань в площині безпеки кінцевого користувача механізми інформаційної безпеки виконують такі завдання.

Механізм керування доступом гарантує, що лише авторизовані користувачі та пристрої отримують доступ та використовують мережне-базовані застосування.

Механізм автентифікації забезпечує перевірку ідентичності (справжності) користувача або пристрою, який намагається мати доступ або використати мережне-базоване застосування. Методи автентифікації можуть бути необхідні як частина керування доступом.

Механізм неспростовності причетності до обміну забезпечує отримання ідентифікаційного запису щодо кожного користувача або пристрою, який має доступ або користується мережне-базованим застосуванням, та щодо дій, які було виконано. Цей запис має бути використано як доказ доступу та використання застосування кінцевим користувачем або пристроєм.

Механізм конфіденційності даних забезпечує захист даних кінцевих користувачів (наприклад, номери кредитних карток користувачів) від неавторизованого доступу або перегляду (ознайомлення) при транспортуванні даних, при їх обробці або при зберіганні у мережне-базованому застосуванні. Те саме стосується даних користувача, які передаються від користувача до мережне-базованих застосувань. У забезпечення конфіденційності даних кінцевого користувача можуть вносити вклад методи, застосовані для керування доступом.

Механізм забезпечення безпечності з'єднання гарантує, що дані кінцевого користувача, які існують при транспортуванні, при обробці або при зберіганні у мережне-базованому застосуванні та дані про самого користувача, оскільки вони передаються від користувача до мережне-базованого застосування, не піддаються не авторизованого доступу, не відхиляються від маршруту або не перехоплюються протягом передачі між даними кінцевими пунктами (прикладом може бути захист від перехоплення телефонних переговорів при радіо доступі).

Механізм забезпечення цілісності даних забезпечує захист даних кінцевого користувача, які існують при транспортуванні, обробці або зберіганні у мережне-базованому застосуванні та дані про самого користувача, оскільки вони передаються від користувача до мережне-базованого застосування, від неавторизованої модифікації, видалення, створення даних та їх копіювання.

Механізм забезпечення доступності даних гарантує, що авторизованому кінцевому користувачу або пристрою не може бути відмовлено у доступі до мережне-базованого застосування. Цей механізм включає захист від активних атак, таких як відмова в обслуговуванні (Denial of Service - DoS), а також як захист від пасивних атак типу модифікації або стирання інформації автентифікації користувача (наприклад, ідентифікаторів і паролів користувача).

Механізм забезпечення приватності гарантує, що мережне-базоване застосування не постачає

неавторизованим особам або пристроям інформацію, яка стосується використання застосування кінцевими користувачами (наприклад, відвідування WEB сторінок). Розкриття цього типу інформації здійснюється лише законному уповноваженому персоналу при наявності ордера на обшук.

Механізми забезпечення приватності в кожному з дев'яти модулів безпеки виконують такі завдання.

На рівні безпеки інфраструктури в площині безпеки менеджменту та в *площині безпеки сигналізації і контролю* гарантується, що інформація, яку можна використати для ідентифікації мережного обладнання або каналів зв'язку, недоступна для неавторизованих суб'єктів або пристроїв. Приклади цього типу інформації включають IP-адреси пристроїв мережі або імена доменів DNS. Для прикладу, маючи можливість ідентифікувати пристрої мережі або канали зв'язку, можна одержати інформацію для планування атак. Захист в площині менеджменту на рівні інфраструктури стосується захисту операцій функціонування, адміністрування, технічного обслуговування та забезпечення (OAM&P) індивідуальних елементів мереж, ліній зв'язку, та серверних платформ, з яких складається мережа. Сюди входить конфігурація апаратури мережі та ліній зв'язку, яка забезпечує дії менеджменту. Прикладом менеджменту інфраструктури, яка повинна бути захищеною, є конфігурація індивідуальних маршрутизаторів або комутаторів, які обслуговуються персоналом мережі. Захист в площині сигналізації та контролю (технологічного керування мережею) рівня інфраструктури полягає у захисті контрольно-сигнальної інформації, яка розміщена в елементах мережі, та серверних платформах, з яких складається мережа, а також як забезпечення захисту прийому та передачі контрольно-сигнальної інформації в мережі, елементах та платформах надавання послуг службами. Наприклад, таблиці комутації, які розміщені у мережних комутаторах, мають бути захищені від втручання або неавторизованого розкриття. В іншому прикладі, маршрутизатори мають бути захищені від прийому або розповсюдження підроблених оновлень маршрутизації або реагування на підроблені запити маршрутизації, створені підробленими маршрутизаторами.

На рівні безпеки інфраструктури в площині безпеки кінцевого користувача гарантується, що елементи мережі не надають неавторизованим суб'єктам або пристроям інформацію, яка може стосуватись мережної діяльності кінцевого користувача (наприклад, географічне місце розташування користувачів, відвіданих web-сторінок тощо). Захист площини кінцевого користувача на рівні інфраструктури складається із захисту даних користувача і голосу, оскільки вони знаходяться або транспортуються через елементи мереж, а також у той час, коли вони транспортуються каналами зв'язку. Захисту проти незаконного перехоплення підлягають також дані користувача, що знаходяться на серверній платформі, оскільки вони транспортуються елементами мережі та каналами зв'язку.

Захист рівня безпеки послуг ускладнений тим фактом, що послуги можуть залежати одна від іншої, щоб задовольнити вимоги клієнта. Для прикладу, щоб забезпечити службу VoIP, провайдер послуги повинен спочатку забезпечити основні (базові) IP служби, які дають змогу забезпечити служби такі як, AAA, DHCP, DNS тощо. Провайдер послуги повинен, таким чином, розгорнути службу VPN, щоб задовольнити якість обслуговування клієнта QoS і вимоги до безпеки для служби VoIP. Тому такі послуги повинні бути розкладені на складові послуги, щоб забезпечити їх повну безпеку.

На рівні безпеки послуг в площині безпеки менеджменту гарантується, що інформація, яку можна використати для ідентифікації систем адміністрування та менеджменту мережних служб, недоступна для неавторизованих суб'єктів або пристроїв. Приклади цього типу інформації включають IP-адреси систем або імена доменів DNS. Наприклад, наявність здатності ідентифікувати систему адміністрування мережних служб може надати інформацію для планування атак. Захист площини менеджменту на рівні послуг стосується безпеки функцій OAM&P мережних служб, а також конфігурації мережних служб, що забезпечують діяльність менеджменту. Прикладом менеджменту служби, яка має бути захищена, є забезпечення обслуговування авторизованих користувачів IP-послуги персоналом мережі

На рівні безпеки послуг в площині безпеки контролю та сигналізації гарантується, що інформація, яку можна використати для ідентифікації мережних пристроїв або каналів зв'язку та які утворюють мережну службу, недоступна для неавторизованих суб'єктів або пристроїв. Приклади цього типу інформації включають IP-адреси мережних пристроїв або імена доменів DNS. Здатність ідентифікувати мережні пристрої або канали зв'язку може надати нападаючому зловмиснику інформацію для планування атак. Захист площини сигналізації та контролю рівня послуг полягає у захисті контрольно-сигнальної інформації, яка використовується мережною службою. Для прикладу, захисту підлягає протокол SIP, який використовується для ініціації та підтримання сеансу VoIP.

На рівні безпеки послуг в площині безпеки кінцевого користувача гарантується, що мережна служба не забезпечує неавторизованим суб'єктам або пристроям інформацію, яка має відношення до використання служби кінцевим користувачем (наприклад, групи викликів для служби VoIP). Захист площини кінцевого користувача на рівні послуг полягає у захисті даних і голосу користувача при використанні мережної

служби. Для прикладу, у службі VoIP повинна бути захищена конфіденційність переговорів користувачів. Аналогічно, служба DNS повинна гарантувати конфіденційність використання служби.

На рівні безпеки застосувань в площині безпеки менеджменту гарантується, що інформація, яка може бути використана для ідентифікації мережне-базованого застосування системи адміністрування або менеджменту, не доступна неавторизованим суб'єктам або пристроям. Захист площини менеджменту на рівні застосувань полягає у захисті функцій OAM&P для мережне-базованих застосувань, конфігурації мережне-базованих застосувань, а також виконання менеджменту в них. Для застосування e-mail, наприклад, при виконанні менеджменту повинні бути захищеними процедури забезпечення і адміністрування поштових скриньок користувача.

На рівні безпеки застосувань в площині контролю та сигналізації гарантується, що інформація, яка може бути використана для ідентифікації мережного пристрою або лінії зв'язку, що використовується у мережне-базованому застосуванні, не доступна неавторизованим особам або пристроям. Захист площини сигналізації та контролю рівня застосувань полягає у захисті контрольно-сигнальної інформації, яка використовується у мережне-базованих застосуваннях. Для прикладу, захисту підлягають протоколи SMTP та POP, які використовуються при керуванні прийманням електронної пошти.

IV Оцінка варіантів розподілу механізмів інформаційної безпеки

Архітектура інформаційної безпеки може застосовуватись під час оцінки безпеки для досліджень необхідності і достатності використаних на рівнях кожної з площин механізмів інформаційної безпеки, повноти запровадження політики безпеки та оцінки степені загальної захищеності телекомунікаційної мережі. В кожному з модулів безпеки можуть комбінуватись механізми безпеки, які забезпечують різну степінь захищеності. Інтегральної оцінки рівня захищеності на сьогодні не сформовано. Не всі показники рівня захищеності мають кількісні оцінки. Показники, які залежать від антропогенних впливів, здебільшого мають якісні оцінки у порядкових шкалах, здобутих методом експертного опитування. Показники захищеності являють собою систему взаємозв'язаних і взаємозалежних компонентів. Оцінка степені захищеності окремих об'єктів телекомунікацій – вузлів, станцій, маршрутизаторів, серверів – є складною задачею, яка виконується експертами. Дослідження у області експертних систем [9, 12, 13] показали ефективність застосування для вирішення таких задач інтелектуальних систем підтримки прийняття рішень, заснованих на експертних знаннях. Об'єктивні оцінки захищеності мереж замінюються експертними оцінками, основаними на евристичних надаваннях переваг. Робота експертних систем заснована на знаннях, які зберігаються у пам'яті системи. Але необхідні розробки моделей та алгоритмів експертних систем підтримки прийняття рішень з оцінки рівня захищеності мереж загального користування, а також продовження розробки програмних систем підтримки професійної діяльності у цій області.

Для подання знань у експертній системі підтримки прийняття рішень по оцінці варіантів розподілу механізмів інформаційної безпеки з використанням нечіткої логіки та нечітких множин можна запропонувати мережну конструкцію, яку задається у вигляді

$$C = <X_{11}, \ldots, X_{ij}; R_1, \ldots, R_k; G> \quad (1)$$

де: – множина об'єктів телекомунікаційної мережі (вузлів, каналів) потужністю i, в кожному з об'єктів якої виділяються $j = 9$ модулів безпеки (три площини безпеки по три рівня в кожній площині); $R_1, \ldots, R_i$ – множина типів зв'язків між об'єктами; G – відображення, яке задає зв'язки між об'єктами X із заданого набору зв'язків. Відповідна експертна система подається у вигляді трьох взаємо пов'язаних моделей: об'єктної моделі, яка відображає дані щодо структурних аспектів мережі; динамічної моделі, яка описує роботу об'єктів мережі; функціональної моделі, у якій розглядається взаємодія між об'єктами. База знань експертної системи складається з теоретичного матеріалу з проблем побудови телекомунікаційних мереж та СЗІБ в ній, а також специфічної експертної інформації, необхідної для підтримки прийняття рішень. Прийняття рішень щодо раціонального вибору варіантів і оцінки захищеності мереж виконується за допомогою правил вирішення. Кожне правило базується на інформації, отримуваної від експерта. За допомогою правил вирішення проводиться часткове впорядкування (ранжирування) точок простору вхідних показників.

Для оцінки степені захищеності мереж методами нечіткої логіки та нечітких множин вводяться лінгвістичні змінні: r – степінь захищеності інформаційного ресурсу, яка забезпечується механізмом інформаційної безпеки у модулі безпеки компонента мережі; s – степінь ризику (ймовірність) здійснення загрози на протязі певного проміжку часу; p – величина можливих збитків, які можуть бути нанесені оператору внаслідок реалізації загроз. Для оцінки ймовірності загрози вводяться декілька дискретних степенів (градацій). Лінгвістичні змінні приймають терм-множину значень T_p, T_r і T_s відповідно

$$T_p = T_r = T_s = \{\text{“незначна”, “низька”, “середня”, “висока”}\}. \quad (2)$$

Границі між значеннями змінних розмиті. Функції приналежності різних термів пересікаються. Значення змінних у кожному конкретному випадку визначається експертним методом або емпіричним шляхом, на основі досвіду експлуатації подібних систем, шляхом реєстрації певних подій, визначення частоти їх повторення тощо. Величина можливих збитків визначається розміром фінансових втрат або, у випадку неможливості їхнього визначення, по якісній шкалі. Наприклад, величина збитків може бути - "відсутня", "низька", "середня", "висока", "недопустимо висока". Дослідження степені захищеності мереж проводять по правилам, які формуються не основі експертного опитування. Основна ідея цього методу полягає у наступному: експертні оцінки задаються у вигляді рівнянь призначення – нечітких відношень, які містять обмеження на базові змінні. Вхідні нечіткі інструкції можуть бути подані деякою комбінацією вхідних правил. Ці рівняння вирішуються відносно бажаних обмежень за допомогою композиції нечітких відношень. Економічна частина цільових функцій має задаватись виходячи з того принципу розумної достатності, згідно якого витрати на інформаційну безпеку $B_{ІБ}$ мають бути менші за можливі збитки $B_З$ за реалізації загроз: $B_{ІБ} < B_З$ [5]. Нечітку базу даних представляють у вигляді:

$$\bigvee_{l=1}^{k_j}[\prod_{i=1}^{n}\left(x_i = a_i^{jl}\right)] \to y = d_j; j = \overline{1,m}; i = \overline{1,n}. \qquad (3)$$

де: a_i^{jl} – нечіткий терм, яким оцінюється вхід x_i; вихід y оцінюється нечітким термом d_j; n – кількість входів; m – кількість термів, які використовуються для лінгвістичної оцінки вихідних даних; входів; k – кількість вхідних правил.

Логічне виведення базується на відомому алгоритмі виведення у нечітких експертних системах [14]. У відповідності з алгоритмом база знань подається у вигляді таблиць, де у стовбцях присутні базові значення лінгвістичних змінних r, s, p тощо та їх модифікації, створені логічними зв'язуваннями "і" "або". З метою використання колективних знань база знань формується шляхом опитування декількох експертів. Для об'єднання індивідуальних суджень у колективне застосовують нечітке відношення "поміж", значення якого подається інтервалом значень на відрізку [0, 1]. Поняття "поміж" у просторі надавання переваг є формалізацією умови Парето для принципу узгодження відношень індивідуального надавання переваг типу: "якщо всі індивідууми надають перевагу об'єкту a перед об'єктом b, то і у груповому надаванню переваг об'єкт a повинен бути кращим об'єкта b". Модель дії експерта при оцінці системи забезпечення інформаційної безпеки та методи формування колективної думки експертів подані в [9].

Якість оцінки захищеності мережі прямо зв'язано з повнотою моделі, яка повинна бути максимально докладною, але простою і компактною. Задовільність деякого правила вирішення можна з'ясувати лише в процесі його застосування. Тому процедура вибору повинна бути кілька кроковою. Якщо правило вирішення не забезпечує визначеності впорядкування варіантів, то на наступному кроці має бути отримана додаткова інформація і побудоване більш "сильне" правило вирішення, яке дозволило б усунути невизначеність впорядкування варіантів. Інформацію, отримувану від експерта необхідно перевіряти на змістовність, адекватність задачі і не суперечливість. Додаткова інформація на кожному кроці повинна порівнюватись із отриманою раніше. Тому процедура побудови правил вирішення повинна бути інтерактивною.

Задача оцінки комплексної СЗІБ, розгорнутої на телекомунікаційній мережі є суттєво складною. Така задача є творчою, базується на емпіричному досвіді фахівців, а ефективність результатів визначається наявністю відповідних знань та досвіду фахівців. При побудові системи оцінки необхідно узгодити між собою низку протилежних принципів, які повинні в такого роду системі працювати разом: принцип зменшення потоку інформації, який має доставлятись людині для прийняття рішення; принцип об'єктно-орієнтованого моделювання при побудові картини предметної області; принцип динамічної структури; принцип повноти інформаційного простору; принцип інтеграції інформаційного простору; принцип децентралізації інформаційного сховища та принцип компонентного складання прикладних режимів.

Рішення експертної системи може бути правильним з деякою ймовірністю. Якщо експертна система має 300 і більше параметрів, вона починає працювати сама на себе [15]. Збільшення кількості нечітких параметрів може приводити до зменшення показників переваги при відборі рішень. Починаючи з деякого порогу вихідні рішення стають слабо розрізненими. Подолання складності сучасних мереж, в даному випадку, можливе за рахунок розробки ієрархічної системи оцінок захищеності мережі. Спочатку оцінюється захищеність модулів безпеки систем, у яких застосована певна множина механізмів інформаційної безпеки. Укрупнені показники оцінки захищеності модулів безпеки використовуються для оцінки захищеності об'єктів мережі: вузлів, станцій, комутаторів тощо. І нарешті, оцінюється захищеність інформаційних ресурсів телекомунікаційної мережі в цілому.

Один із законів складних систем полягає у тому, що оптимальні показники захищеності ресурсів складної системи можуть досягатись тоді, коли функціонування механізмів захисту компонентів складної

системи не буде оптимальним. Оптимальною величиною захищеності ресурсів системи є така, яка досягається за мінімальних витрат, які мають бути меншими ніж можливі втрати від реалізації загроз, яким протистоїть СЗІР. У [16] оптимальною системою захисту інформації називається така система захисту, яка забезпечує максимальну степінь захищеності при мінімальному потенційному збитку, максимальній функціональності та продуктивності інформаційної системи (максимумі функцій інформаційної системи та мінімумі середнього часу доступу до об'єктів захисту інформаційної системи). На функціонування механізмів та сервісу інформаційної безпеки витрачаються ресурси телекомунікаційної мережі: час, програмне та апаратне забезпечення, збільшується навантаження мережі та час затримки повідомлень, зменшується пропускна здатність телекомунікаційної мережі. Роль експертної системи прийняття рішень полягає у пошуку компромісу. Механізми інформаційної безпеки повинні нормально функціонувати у кожному модулі безпеки і, при цьому, не заважати роботі інших компонентів СЗІБ телекомунікаційних мереж.

Ще одну проблему складають питання довіри до значень вхідних змінних та коректності бази знань, яка повинна бути побудована на основі експериментально підтверджених матеріалів щодо побудови та функціонування СЗІБ телекомунікаційних мереж. Автори вважають необхідним проводити широкі експериментальні дослідження – вести накопичування, документування і використання результатів регулярного моніторингу інформаційної безпеки для вдосконалення і розвитку системи оцінки інформаційної безпеки та одержання статистики технічної експлуатації СЗІБ.

Висновки

Результати аналізу розподілу механізмів інформаційної безпеки можуть бути використанні при проектуванні СЗІБ телекомунікаційних мереж загального користування (МЗК) та організації її технічної експлуатації. Але необхідні розробки моделей та алгоритмів експертних систем підтримки прийняття рішень з оцінки рівня захищеності мереж загального користування, продовження розробки програмних систем підтримки професійної діяльності у цій області, а також використання результатів постійного моніторингу інформаційної безпеки МЗК. Напрямками подальшого дослідження можуть бути розробка методик оцінки ефективності СЗІБ МЗК та відповідних техніко-економічних обґрунтувань.

*Література: **1**. Закон України "Про телекомунікації" (від 18. 11. 2003 р). **2.** Тардаскін М. Ф., Кононович В. Г. Правові засади інформаційної безпеки телекомунікаційних мереж // "Зв'язок", № 4, 2004. С. 35 - 38. **3.** Кононович В. Г. Тардаскін М. Ф., Тардаскіна Т. М. Аналіз проблеми розподілу витрат на інформаційну безпеку інформаційно-телекомунікаційних систем. "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 8, 2004. С 62 - 68. **4.** Хорошко В., Ковальова Ю., Плус Д. Розподіл ресурсів у багато рубіжній системі захисту. "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 8, 2004. С. 39 - 43. **5.** Кононович В. Г., Тардаскіна Т. М. Алгоритм розподілу ресурсів інформаційної безпеки документальних телекомунікацій. "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 9, 2004. С 152 - 161. **6.** ITU-T Recommendation X.200. Reference model of open systems interconnection for CCITT applications. Geneva. 1991. С. 75; (Стандарт ISO 7498-1:1984. Базова модель ВВС). **7.** ITU-T Recommendation X.800. Security architecture for Open Systems Interconnection for CCITT applications. Geneva.1991. С.48; (Стандарт ISO 7498-2: 1989. Архітектура безпеки ВВС). **8.** ITU-T Recommendation X.805. Security architecture for system providing end-to-end communications. С. 28. **9.** Потій О., Лєншин А. Методика визначення думок експертів відносно зрілості безпеки інформації із застосуванням математичного апарату суб'єктивної логіки. "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 9, 2004. С. 38 - 47. **10.** Ліцензійні умови провадження діяльності у сфері телекомунікацій з надання послуг фіксованого міжнародного міжміського, місцевого зв'язку з правом технічного обслуговування та експлуатації телекомунікаційних мереж і надання в користування каналів електрозв'язку" (наказ Держкомзв'язку № 132 від 17. 06. 2004 р.), С. 25. **11.** Ліцензійні умови провадження діяльності у сфері телекомунікацій з технічного обслуговування і експлуатації мереж ефірного теле- та радіомовлення та телемереж, надання в користування каналів електрозв'язку" (наказ Міністерства транспорту та зв'язку України № 984 від 10. 11. 2004 р.) С. 20. **12.** Шорошев О. Оцінка стану безпеки інформації за стандартними профілями її захищеності в комп'ютерних (автоматизованих) системах. "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 8, 2004. С. 48 - 56. **13.** Маренко В. А. Модели и алгоритмы экспертных систем поддержки принятия решений по электромагнитной совместимости. Автореферат диссертации. Тюмень, 2004. С. 18. **14.** Домарев В. В. Математические модели систем и процессов защиты информации. http://www.domarev.kiev.ua/nauka/. С. 56. **15**. Кравченко В. П. Система поддержки принятия решений. http://it2b.ru/it2b2.viev5.page21.html.*

16. *Носов В., Манжай А. Метод проектирования оптимальной системы защиты информации. "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 8, 2004. С. 94 - 103.*

УДК 621.396.6

ВЫБОР ПАРАМЕТРОВ И ПОСЛЕДОВАТЕЛЬНОСТИ ИХ ИЗМЕРЕНИЯ ПРИ ТЕХНИЧЕСКОМ ОБСЛУЖИВАНИИ АППАРАТУРЫ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ ПО СОСТОЯНИЮ

Лев Сакович, Руслан Бобро
Спецфакультет СБ Украины в составе ВИТИ НТУУ «КПИ»

Анотація: **Отримані аналітичні вирази з кількісної оцінки ймовірності переважного вибору параметрів при технічному обслуговуванні апаратури систем захисту інформації за станом, а також формалізовано порядок визначення параметрів і послідовність їх вимірювання.**
Summary: **The analytical expressions for a quantitative estimation of probability of a preferable choice of parameters had been received at maintenance service of the equipment of systems of protection of the information on a condition, and also the order of definition of parameters and sequence of their measurement had been formalized.**
Ключевые слова: **Техническое обслуживание по состоянию, аппаратура систем защиты информации, вероятность предпочтительного выбора.**

I Введение и постановка задачи

Поддержание требуемого уровня надежности элементов и систем – одна из основных задач по обеспечению высокой безопасности и живучести сложных технических систем. Среди мероприятий по повышению надежности при эксплуатации оборудования сложных систем важное место отводится техническому обслуживанию [1].

Под техническим обслуживанием (ТО) аппаратуры систем защиты информации понимается комплекс операций или операция по поддержанию исправности или работоспособности изделий при их технической эксплуатации. Вид ТО определяется по одному из признаков: этапу эксплуатации, периодичности, объему работ, условиям эксплуатации или другим. Система ТО изделий – совокупность взаимосвязанных средств, исполнителей и документации, предназначенная для поддержания и восстановления их исправного или работоспособного состояния [2].

При эксплуатации аппаратуры систем защиты информации устанавливаются следующие виды ТО [3]: периодическое (календарное, по наработке); комбинированное; непериодическое (по состоянию). Во всех случаях выполняется проверка параметров обслуживаемых изделий на соответствие техническим условиям.

Работы по ТО сложных систем в процессе эксплуатации можно осуществлять двумя способами: проводить регулярно или сначала измерять значения некоторых параметров, изменяющихся под воздействием внешних дестабилизирующих факторов и старения, а затем решать вопрос о проведении необходимых работ в зависимости от фактического состояния системы. Организация такого вида ТО получила название эксплуатации по состоянию. В этом случае необходимо использовать более полную информацию о состоянии объекта, чем при календарном ТО, основанном на информации только о моментах отказов [1].

Важнейшим преимуществом внедрения ТО по состоянию является минимизация времени, трудозатрат и средств на его проведение без ухудшения эффективности функционирования обслуживаемой системы [4, 5]. Благодаря указанным достоинствам ТО по состоянию рекомендовано использовать в процессе эксплуатации сложных систем, к которым относятся и средства защиты информации (СЗИ).

При организации эксплуатации СЗИ по состоянию возникают следующие задачи [1]:

- выбор минимально необходимого числа контролируемых параметров, несущих достаточную информацию о состоянии объекта в любой момент времени;
- обоснование допустимых областей изменения выбранных для контроля параметров;
- разработка алгоритмов математического обеспечения для обоснования программ эксплуатации по состоянию;