УДК 621.391.41

Власов О. М., *д.т.н.*; **Толюпа С. В.,** *д. т. н.*

КОМПЛЕКСНИЙ ПІДХІД ОЦІНКИ ЕФЕКТИВНОСТІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ НОВОГО ПОКОЛІННЯ

Власов О. М., Толюпа С.В. Комплексний підхід оцінки ефективності систем захисту інформації в інфокомунікаційних мережах нового покоління. В статті розглядається питання гарантування безпеки інформації в мережах нового покоління на основі комплексного підходу. Такий підхід відповідає комплексному характеру завдання забезпечення безпеки мереж телекомунікацій на всіх етапах їх життєвого циклу – від концептуальних схем та проектування до технічної експлуатації та використання.

Ключові слова: МЕРЕЖА НОВОГО ПОКОЛІННЯ, ЗАХИСТ ІНФОРМАЦІЇ, ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Власов А. Н., Толюпа С. В. Комплексный подход оценки эффективности систем защиты информации в инфокоммуникационных сетях нового поколения. В статье рассматривается вопрос обеспечения безопасности информации в сетях нового поколения на основе комплексного подхода. Такой подход соответствует комплексному характеру задачи обеспечения безопасности сетей телекоммуникаций на всех этапах их жизненного цикла – от концептуальных схем и проектирования до технической эксплуатации и использования.

Ключевые слова: СЕТЬ НОВОГО ПОКОЛЕНИЯ, ЗАЩИТА ИНФОРМАЦИИ, ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Vlasov O. M., Tolyupa S. V. A comprehensive approach for evaluating of efficiency of information security systems in NGN infocommunication systems. The paper considers the issue of providing information security in the next generation networks on the basis of comprehensive approach. This approach corresponds to the complex nature of the task for providing security for telecommunication networks at all stages of their life cycle – from conceptual planning and designing to maintenance and application.

Key words: NEXT GENERATION NETWORK, INFORMATION SECURITY, INFORMATION TECHNOLOGY

На сьогоднішній день ми можемо спостерігати соціальні зміни в галузі телекомунікацій, які принесли із собою доктрини мереж нового покоління. Зміни помітні не лише за характером публікацій, а і за рівнем спілкування між фахівцями. Навіть поверхневий погляд виявить, що сучасне зв'язкове співтовариство розділилося на дві частини: одна дотримується традиційних принципів, а інша вже живе в мережах нового покоління.

Впровадження мереж нового покоління не можна звести до механічної заміни однієї технології іншою, що було в історії мереж зв'язку неодноразово. Ми дійсно маємо справу зі зміною парадигми та зі справжньою революцією, що супроводжують зміни, хаос ідей, ламання світогляду і все те, що робить сучасний етап технічної історії унікальним і особливо цікавим для дослідження

Демократичність мереж нового покоління проявляється на всіх рівнях і у всіх рішеннях. Прикладом може служити технологія *Softswitch*, де ми маємо подвійність. З одного боку, це певний вузол у складі мережі, закінчений мережний елемент, з іншого боку – концепція побудови рівня управління в мережі. Така ж подвійність присутня в *Triple Play*. З одного боку, це концепція універсалізації послуг, що передбачає розкладання окремої послуги на три, з іншого боку – окрема послуга, одна серед багатьох послуг мереж майбутнього. Така подвійність також є наслідком демократичності концепції мереж нового покоління. Принцип демократичності не обмежується тільки технічною стороною, його сліди можна знайти на всіх етапах життя мереж майбутнього. Розробка, будівництво, принципи організації й експлуатації мереж також перетерплюють зміни відповідно до принципу демократичності.

Для мереж нового покоління характерне сполучення принципів децентралізованого керування й децентралізованого функціонування окремих елементів. Якщо комп'ютер стає головним елементом користувача мереж наступного покоління, то природно використовувати комп'ютери як інтелектуальні пристрої в різних вузлах мережі й створювати на основі мікропроцесорів окреме устаткування. Таким чином, мережі

майбутнього – це мережі розподіленого машинного інтелекту. Вибір між централізованим і розподіленим (децентралізованим) принципами керування системами в багатьох випадках складний. Але одне можна затверджувати виразно: розподілені системи більш стабільні й здатні деякою мірою коректувати збої в мережі. Друга перевага систем розподіленого інтелекту – вони здатні гнучко підлаштовуватись до змін навколишнього середовища.

Проблема багатьох систем зв'язку зводиться до того, що кількість параметрів, необхідних для опису поводження системи зв'язку (розмірність системи), виявляється дуже великою і прийняти правильне рішення в таких мережах досить складно, враховуючи, що інформація про стан мережі може бути досить суперечливою. Збільшення розмірності сучасної технології представляється об'єктивною тенденцією, яку можна спостерігати в історичному зрізі протягом усього розвитку цифрових мереж зв'язку [1].

Поява концепції мереж нового покоління (*NGN* та *FN* – мереж майбутнього) дозволить операторам значно розширити горизонти своєї діяльності, спектр послуг. Проте шлях переходу до мереж, на базі яких можливе надання мультисервісних послуг, складний і тернистий. Тому ставиться питання, чи не простіше продовжувати експлуатувати існуючі мережі, поки є попит на перелік послуг, що вже склався і піклуватися про їх якість.

Безумовно в стрімкому розвитку мереж нового покоління можна назвати і "больові точки" експлуатації інфокомунікаційних мереж нового покоління з погляду оператора**.** Ключові моменти в експлуатації мережі – її надійність і досконаліть системи управління. До "больових точок" експлуатації мереж нового покоління можна віднести не стільки проблеми із застосовуваними технологіями, скільки завдання забезпечення стійкої роботи мережевого устаткування, стиковка протоколів і інтерфейсів різних постачальників. Одне з основних завдань мережі нового покоління – забезпечення інформаційної безпеки.

Гарантування безпеки інформації в мережах нового покоління взагалі та їх системах управління є складним комплексним завданням. У міжнародних стандартах проблеми захисту інформації вирішуються одночасно зі стратегічними та конкретними питаннями розвитку архітектури мережі.

Такий підхід відповідає комплексному характеру забезпечення безпеки мереж телекомунікацій на всіх етапах їх життєвого циклу – від концептуальних схем та проектування до технічної експлуатації та використання. Окремими заходами досягти мети, як правило, не вдається й тому в кожному випадку потрібно розглядати всю систему в комплексі, причому захищеність усієї інфокомунікаційної системи (мережі) визначається рівнем захищеності її найбільш слабкої частини.

Проблема захисту інформації стає ще більш актуальною з розвитком інтелектуальних мереж, коли користувач отримує можливість більш широкого доступу до ресурсів мережі, у тому числі отримує можливість управляти цими ресурсами. Усе це зумовлює можливість несанкціонованого доступу та несанкціонованих дій.

Загальноприйнятою у світі є класифікація ступеня захищеності інформаційної системи за такими рівнями безпеки:

D – рівень мінімального захисту (Manimal Protection). Зарезервовано для систем, які одержали попередню оцінку, однак для класифікації за іншими рівнями не забезпечують потрібного рівня безпеки;

C_1 – рівень вибіркової безпеки (Discretionary Protection). Дає змогу користувачам застосовувати обмеження доступу для захисту приватної інформації;

C_2 – рівень доступу, що управляється (Controlled Access Protection). Містить вимоги рівня C_1, а також вимоги до захисту процесу реєстрації в системі, обліку подій захисту, ізоляції ресурсів різних процесів;

B_1 – рівень захисту за категоріями (Labeled Protection). До вимог рівня C_2 додається можливість захисту окремих файлів, записів у файлах, інших об'єктів системи спеціальними

позначками безпеки, що зберігаються разом із цими об'єктами; вважається, що подолання такого захисту потребує дуже високої підготовки;

B_2 – рівень структурованого захисту (Structured Protection). До вимог рівня B_1 додається повний захист усіх ресурсів системи;

B_3 – рівень доменів безпеки (Security Domains). До вимог рівня B_2 додається явна специфікація користувачів, яким заборонено доступ до певних ресурсів, повніша реєстрація потенційно небезпечних подій. Вважається, що навіть дуже досвідчені програмісти не спроможні подолати систему з таким рівнем безпеки;

A_1 – рівень верифікованої розробки (Verified Design). Забезпечується повний захист інформації, застосовуються специфіковані та верифіковані механізми безпеки. Цей рівень безпеки вважається найвищим.

У кожній інформаційній системі можна виділити найслабкіші з погляду безпеки місця. На них необхідно звернути увагу передусім. До таких місць, звичайно, належать сховища даних, адміністративна система, кабельна система, система доступу із зовнішніх мереж. Зловмисник, знайшовши доступ до сховища даних, зможе взяти з нього конфіденційні дані, а зайшовши в адміністративну систему, він матиме доступ до всіх ресурсів системи. До кабельної системи завдяки її розгалуженості легко приєднатися, підслухати та проаналізувати дані, що передаються, або підмінити їх іншими [2].

Найпростіше описати механізм надання та обмеження прав доступу з використанням таблиці правомірності, яка ставить у відповідність певній категорії об'єктів операційної системи права доступу до інформації (переглядання, читання, створення, записування тощо). Такими об'єктами можуть бути: окремі користувачі, групи користувачів, рівень таємності, прикладні програми, час доби, робоча станція, довільна комбінація названих об'єктів.

Забезпечення захисту інформації в інфокомунікаційних системах та мережах (ІКСМ) відбувається в умовах випадкової дії різних чинників, частина з яких є систематизованими в стандартах, а частина наперед невідомі. Оцінка ефективності систем захисту інформації (СЗІ) повинна обов'язково враховувати як об'єктивні обставини, так і ймовірнісні фактори, а її характеристики повинні мати ймовірнісний характер. Особливу важливість на сучасному етапі розвитку інформаційних технологій (ІТ) має обґрунтовування оптимальних значень показників ефективності та цільове призначення ІКСМ.

Таким чином, виникає проблема оцінки ефективності ІКСМ у цілому та СЗІ, зокрема. Для вирішення цієї проблеми пропонується використовувати комплексний підхід, тому розглянемо основні вимоги до показників і критеріїв оцінки СЗІ.

Слід зазначити, що захист критично важливих ІКСМ відповідає численним міжнародним, національним, корпоративним, нормативним і методичним документам [3...5]. Застосовуються дуже дорогі технічні засоби і впроваджуються суворо регламентовані організаційні заходи. Проте немає адекватної оцінки – наскільки пропоноване або вже реалізоване рішення добре, яка його запланована або реальна ефективність. Такому стану, що склався зараз у проектуванні інформаційних технологій, є ряд причин:

– ігнорування комплексного підходу як методології аналізу й синтезу СЗІ;

– відсутність механізмів повного й достовірного підтвердження якості СЗІ;

– недоліки нормативно-методичного забезпечення інформаційної безпеки, перш за все в області показників і критеріїв.

У роботі [3] викладені основні вимоги до захисту:

– система захисту інформації повинна бути комплексною;

– СЗІ повинна бути пристосована до змінних умов;

– системний підхід до захисту інформації повинен застосовуватися, починаючи з підготовки технічного завдання й закінчуватися оцінкою ефективності і якості СЗІ в процесі її експлуатації.

Перш за все, СЗІ повинна мати цільове призначення. Причому, чим більш конкретно сформульована ціль захисту інформації, детально з'ясовані ресурси, які залучаються для цього, а також визначений комплекс обмежень, тим більшою мірою можна чекати отримання бажаного результату. Якщо ціль забезпечення інформаційної безпеки проста (формулюється скалярним показником) і принципово досяжна, то виявляється достатньо порівняно нескладних по складу й структурі засобів захисту інформації. Проте при розширенні кола проблем забезпечення інтегральної інформаційної безпеки, зміст цільового призначення системи на формалізованому рівні буде мати багатовимірний, векторний характер. При цьому значимість властивостей окремих елементів засобів захисту інформації знижується, а на перший план висуваються загальносистемні задачі – визначення оптимальної структури й режимів функціонування системи, організація взаємодії між її елементами, облік впливу зовнішнього середовища й т. ін. При цілеспрямованому об'єднанні елементів у систему остання буде мати специфічні властивості, спочатку не властиві жодній з її складових частин. При комплексному підході мають першорядне значення тільки ті властивості елементів, які визначають взаємодію один з одним і роблять вплив на систему в цілому, а також на досягнення поставленої мети.

Результативне рішення задач аналізу й синтезу СЗІ не може бути забезпечено одними лише способами наглядного опису їх поведінки в різних умовах – системотехніка висуває проблеми, які вимагають кількісної оцінки характеристик. Такі дані, отримані експериментально або шляхом математичного моделювання, повинні розкривати властивості СЗІ. Основною з них є ефективність, під якою, згідно [4], розуміється ступінь відповідності результатів захисту інформації поставленій цілі. Остання, залежно від ресурсів, що є в наявності, знань розробників і інших чинників, може бути досягнута в тій чи іншій мірі, при цьому можливі альтернативні шляхи її реалізації. Ефективність має безпосередній зв'язок з іншими системними властивостями, у тому числі якістю, надійністю, керованістю, завадостійкістю. Тому кількісна оцінка ефективності дозволяє виміряти й об'єктивно аналізувати основні властивості систем на всіх стадіях їх життєвого циклу, починаючи з етапу формування вимог і ескізного проектування.

СЗІ відповідно до діючих норм і правил підлягають обов'язковій або добровільній сертифікації, але навіть сертифікація не дає необхідних гарантій. У кращому разі перевіряється тільки 85% всіх можливих станів, а реально – 60...70%. Тобто сертифікація продукції на відповідність вимогам державних стандартів по безпеці інформації або інших нормативних документів підтверджується з певним ступенем достовірності. Проте, чому конкретно повинна бути рівна ця достовірність, чи є цей термін еквівалентним ймовірнісно-статистичному розумінню, мова не йде. Тим часом, на випробувальні центри (лабораторії), які проводять дослідження зразків сертифікованої продукції та беруть участь у попередній перевірці її виробництва, прямо покладена відповідальність за достовірність результатів.

Таким чином, навіть якщо елементи СЗІ формально успішно пройшли всі сертифікаційні випробування й мають повний комплект засвідчуючих документів, це ні в якому разі не означає того, що реально буде забезпечений рівень якості, що вимагається.

Труднощі об'єктивного підтвердження ефективності СЗІ полягають у недосконалості існуючої нормативної бази, а також у підходах, що склалися в проектуванні інформаційних технологій, принципово відмінних від розроблених у традиційній інженерії. Слід зазначити недостатню опрацьованість системи показників якості інформаційної безпеки. У незадовільному стані знаходиться система критеріїв безпеки, у тому числі, таких, як ефективність СЗІ. До серйозних проблем відноситься також ігнорування стохастичної природи подій і явищ, які виникають у процесі захисту інформації, абстрагування від їх економічного вмісту в нормативному, методичному та прикладному аспектах [6].

Слід зазначити, що нормативні документи, які оцінюють безпеку інформаційних технологій, практично не містять конкретних методик, внаслідок чого величина розриву між загальними деклараціями й конкретним інструментарієм по реалізації й контролю їх положень є неприпустимою.

Виходячи ж зі свого призначення, методична база повинна охоплювати всі критично важливі аспекти забезпечення й перевірки виконання вимог, що пред'являються до інформаційної безпеки. Об'єктивним видом оцінки ефективності СЗІ є функціональне тестування, яке призначене для перевірки фактичної працездатності реалізованих механізмів безпеки та їх відповідності пред'явленим вимогам, які забезпечують отримання статистичних даних.

Внаслідок того, що засоби безпеки мають обмежені можливості щодо протидії загрозам, завжди існує вірогідність порушення захисту, навіть якщо під час тестування механізми безпеки не були обійдені або блоковані. Для оцінки цієї вірогідності повинні проводитися додаткові дослідження. У методичному плані визначення ефективності СЗІ повинне полягати у виробленні думки щодо придатності способу дій персоналу або пристосованості технічних засобів до досягнення мети захисту інформації на основі вимірювання відповідних показників, наприклад, при функціональному тестуванні.

Ефективність СЗІ оцінюється для вирішення наступних задач:

– ухвалення рішення про допустимість практичного використовування СЗІ в конкретній ситуації;

– виявлення внесків різних чинників у досягнення мети;

– встановлення шляхів підвищення ефективності СЗІ;

– порівняння альтернативних варіантів систем.

Таким чином, при використовуванні сучасної методичної бази, оцінка ефективності СЗІ носить в основному нечіткий, суб'єктивний характер, практично повністю відсутні нормовані кількісні показники, які враховують можливі випадкові або навмисні дії. В результаті достатньо складно, а часто й неможливо, оцінити якість функціонування інформаційної системи за наявності несанкціонованих дій на її елементи, а, відповідно, і визначити, чим один варіант проектованої системи краще за інший. Тому рішенням проблеми комплексної оцінки ефективності СЗІ є використовування системного підходу, який дозволяє ще на стадії проектування кількісно оцінити рівень безпеки й створити механізм управління ризиками. Проте цей шлях може бути реалізований за наявності відповідної системи показників і критеріїв.

Відповідно до сучасної теорії оцінки ефективності систем, якість будь-якого об'єкту, у тому числі й СЗІ, виявляється лише в процесі його використовування за призначенням (цільове функціонування), тому найбільш об'єктивним є оцінювання по ефективності застосування.

Проектування, організація й застосування СЗІ фактично пов'язане з невідомими подіями в майбутньому й тому завжди містять елементи невизначеності. Крім того, присутні й інші причини неоднозначності, такі як недостатньо повна інформація для ухвалення рішень управління або соціально-психологічні чинники. Тому, наприклад, етап проектування СЗІ природним чином супроводить значна невизначеність. В ході реалізації проекту її рівень знижується, але ніколи ефективність СЗІ не може бути адекватно виражена й описана детермінованими показниками. Процедури випробувань, сертифікації або ліцензування не усувають повністю невизначеність властивостей СЗІ або її окремих елементів і не враховують випадковий характер атак.

Тому об'єктивною характеристикою якості СЗІ – ступенем її пристосованості до досягнення рівня безпеки, який вимагається, в умовах реальної дії випадкових чинників, може служити ймовірність, яка характеризує ступінь можливостей конкретної СЗІ при

заданому комплексі умов. Іншими словами – вірогідність досягнення мети операції або вірогідність виконання задачі системою. Ця вірогідність повинна бути встановлена в основу комплексу показників і критеріїв оцінки ефективності СЗІ. При цьому критеріями оцінки служать поняття придатності та оптимальності. Придатність означає виконання всіх встановлених до СЗІ вимог, а оптимальність – досягнення однієї із характеристик екстремального значення при дотриманні обмежень і умов на інші властивості системи. При виборі конкретного критерію необхідно його узгодження з метою, що покладається на СЗІ.

Під час синтезу системи виникає проблема рішення задачі з багатокритерійним показником. При цьому розглядаються показники ефективності, які призначені при рішенні задачі порівняння різних структур СЗІ.

Оцінка оптимального рівня гарантій безпеки в певній мірі залежить від збитку, пов’язаного з помилкою у виборі конкретного значення показника ефективності. Для отримання чисельних оцінок ризику необхідно знати розподіли ряду випадкових величин. Це певною мірою обмежує кількісне дослідження рівнів гарантій безпеки, які надаються СЗІ, але в багатьох практичних випадках такі оцінки можна отримати за допомогою імітаційного моделювання або за наслідками активного аудиту СЗІ.

Формування інтегральної оцінки ефективності СЗІ ІКСМ. На даний час в теорії інформаційної безпеки класифікація задач захисту інформації передбачає їх розподіл на п'ять класів (рис. 1).

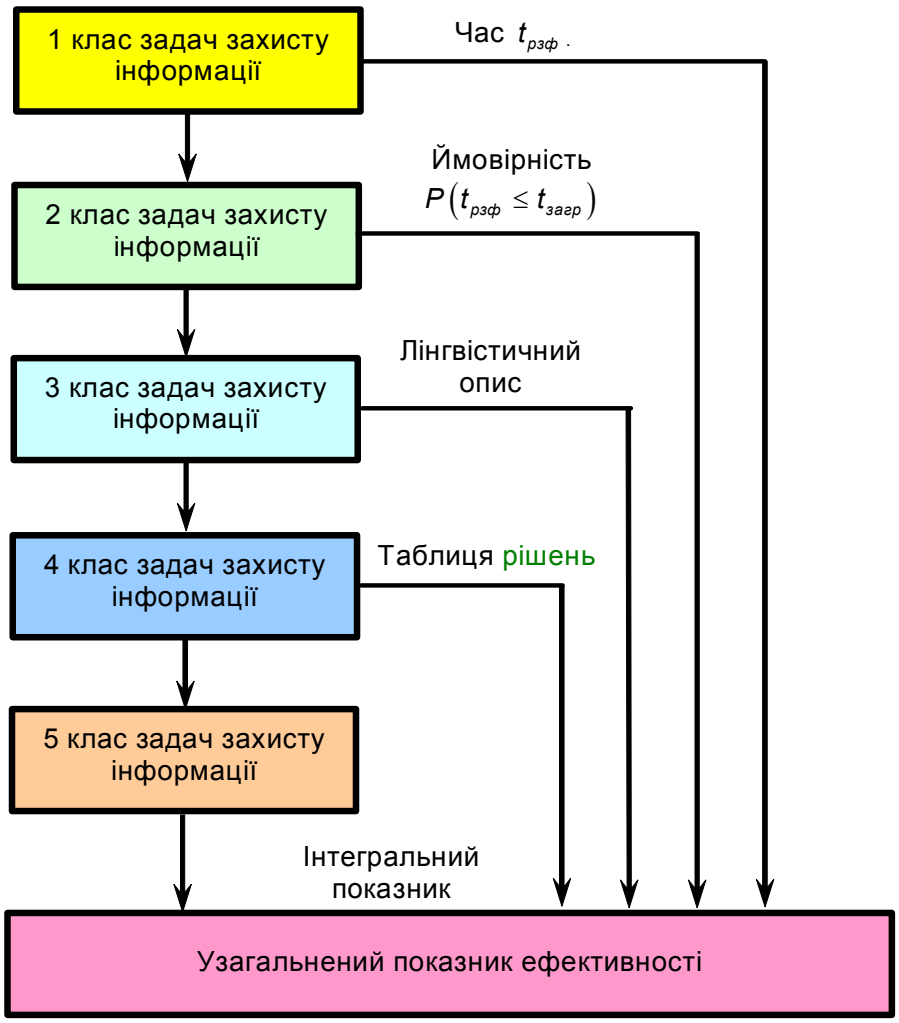

Рис. 1. Формування узагальненого показника ефективності

Перший клас задач описує властивості, пов'язані з можливостями втручання в процес обробки інформації з метою регулювання і реєстрації доступу до засобів обробки інформації в ІКСМ, криптографічного перетворення інформації, контролю і реагування на загрози інформаційної безпеки ІКСМ, а також скриття та імітації випромінювань і наведень. Найдоцільнішою формою показників ефективності захисту інформації при рішенні даного класу задач є час реалізації захисних функцій відповідними засобами.

Другий клас задач описує властивості, які пов’язані з можливостями по попередженню умов появи загроз, пошуку, виявленню й знешкодженню, як самих загроз, так і їх джерел, а також із можливостями по відновленню інформації після дії загроз. Перераховані можливості визначаються своєчасністю реагування засобів і систем захисту інформації на загрози інформаційної безпеки ІКСМ. В якості такого показника доцільно використовувати ймовірність того, що час реалізації захисних функцій не перевищить тривалості відповідних фаз загрози. Очевидно, що цей показник є функцією від тимчасових характеристик, що пов’язує його з показниками ефективності КСЗІ при рішенні першого класу задач захисту інформації.

Третій клас задач описує властивості, пов’язані з можливостями комплексного підходу до захисту інформації (КСЗІ) від несанкціонованого доступу, від витоку за рахунок побічних електромагнітних випромінювань та наведень і від витоку по акустичному каналу. Ці можливості визначаються ступенем відповідності функцій які виконуються по протидії загрозам інформаційної безпеки ІКСМ, якості забезпечення зон захисту КСЗІ, як системи, яка функціонує за призначенням. Найдоцільнішою формою представлення показників даного рівня є опис їх за допомогою лінгвістичних змінних, базові значення для яких визначаються показниками, відповідними ефективності виконання другого класу задач захисту інформації.

Четвертий клас задач описує властивості, пов’язані з можливостями КСЗІ по запобіганню порушення конфіденційності, доступності і цілісності інформації. Показники даного рівня узагальнюють властивості КСЗІ, пов’язані із забезпеченням зон захисту, і можуть бути отримані за допомогою таблиць рішень, у яких як початкові дані використовуються оцінки показників ефективності рішення третього класу задач захисту інформації.

П'ятому класу відповідає властивість КСЗІ, яка характеризує ступінь досягнення цілей його функціонування і являється результатом узагальнення можливостей забезпечення захисту інформації по основних режимах роботи. Відповідний даному рівню показник є інтегральним.

Велика кількість засобів, що входять у КСЗІ, а також відмінність вирішення ними приватних задач захисту інформації ставлять досить складну проблему оцінки ефективності захисту інформації в ІКСМ. Одним із найперспективніших шляхів її рішення в рамках “Загальних критеріїв” є інтеграція приватних показників, засобів захисту інформації, що входять в склад КСЗІ, на основі їх структуризації.

Структуризація заснована на ряді положень. Інтегральний показник ефективності захисту інформації в ІКСМ базується на структурованій сукупності приватних показників ефективності СЗІ.

Структура системи показників ефективності СЗІ, при їх інтеграції представляється у вигляді пірамідальної мережі – як результат поетапного узагальнення властивостей СЗІ, починаючи із приватних і закінчуючи самим узагальненим.

Пірамідальна мережа показників ефективності СЗІ має багаторівневу структуру. Її рівні визначаються виходячи з таких умов:

– кожному рівню відповідає конкретний клас властивостей СЗІ;

– кожен рівень представляє певний ступінь узагальнення властивостей КСЗІ, причому показники нижнього рівня мають найнижчий ступінь узагальнення, а показник верхнього рівня є інтегральним;

– число показників поточного рівня не повинне перевищувати числа показників нижнього по відношенню до даного рівня.

Багаторівневій структурі системи показників ефективності СЗІ відповідає багаторівнева структура форм представлення відповідних показників, які змінюються від кількісної шкали для оцінки показників нижнього рівня до якісної - на верхніх.

Оцінка динамічних характеристик СЗІ здійснюється за допомогою кількісної шкали, статичних – за допомогою якісної шкали.

Існує адекватна система показників ефективності СЗІ – система математичних моделей для їх оцінки. Відповідно до даної вимоги кожному рівню пірамідальної мережі показників ефективності СЗІ ставиться у відповідність певний тип математичних моделей, які забезпечують оцінку показників цього рівня.

Існує уніфікований формальний опис процесів функціонування СЗІ, виходячи з якого, можна отримати будь-який тип математичної моделі, яка відповідає переліку властивостей. Властивості СЗІ виявляються при рішенні відповідних задач захисту інформації.

Таким чином, можна зробити висновок про необхідність оцінки ефективності систем безпеки не тільки по якісних характеристиках, але й по кількісних показниках.

Вдосконалення нормативної бази, методичного забезпечення в області інформаційної безпеки повинно відбуватися, перш за все, у напрямі використовування характеристик вірогідності. Змістовні результати за оцінкою ефективності СЗІ можуть бути отримані тільки при комплексному підході до структуризації приватних показників якості й критеріїв ефективності.

Література

1. Толюпа С. В. Проблемні питання щодо впровадження мереж нового покоління на телекомунікаційному ринку України / С. В. Толюпа // Зб. наук. праць ВІКНУ ім. Тараса Шевченка. – 2010. – № 26. – С. 120-126.

2. Ленков С. В. Методы и средства защиты информации / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко. – К.: Техніка, 2008. – Т. 1. – 465 с.

3. Закон України «Про захист інформації в автоматизованих системах».

4. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу // НД ТЗІ 2.5-004-99.

5. Захист інформації. Технічний захист інформації. Основні положення // ДСТУ 3396.0-96. – К.: Держспоживстандарт України, 1997. – 18 с.

6. Подиновский В. В. Количественная важность критериев / В. В. Подиновский // Автоматика и телемеханика. – 2000. – № 5. – С. 110-123.