УДК 004.621.37

Толюпа С.В., Іванова О.М., Демченко І.О.

ПІДХОДИ ДО ПРОЕКТУВАННЯ ТА ОЦІНКИ ЕФЕКТИВНОСТІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ ОБРОБКИ ТА ПЕРЕДАЧІ ДАНИХ

В статті запропоновано розв’язання проблеми захисту інформації в автоматизованих систем обробки і передачі інформації за рахунок реалізації системного підходу

Ключові слова: автоматизована система, комплексна система захисту інформації, несанкціонований доступ

Соціальні і економічні зміни останніми роками створили умови для широкого впровадження в Україні новітніх інформаційних технологій, створення і використання перспективних інформаційних, телекомунікаційних систем зв'язку, автоматизованих систем обробки і передачі інформації (АСОПІ) як в державному, так і в недержавному секторах [1].

Проте створення індустрії обробки інформації, даючи об'єктивні передумови для грандіозного підвищення ефективності життєдіяльності людства, породжує цілий ряд складних і великомасштабних проблем. Однією з таких проблем є організація захисту інформації, яка циркулює і обробляється в автоматизованих системах обробки та передачі даних. Захист інформації полягає в створенні і підтримці в дієздатному стані системи заходів, як технічних, так і нетехнічних, що дозволяють запобігти або ускладнити можливість реалізації загроз, а також знизити потенційні збитки.

Гарантування безпеки інформації в автоматизованих систем обробки і передачі інформації 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 інформаційних мереж 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 визначається рівнем захищеності її найбільш слабкої частини.

Чисельні публікації останніх років показують, що засоби здобування (заволодіння) інформації, яка циркулює в автоматизованій системі обробки та передачі даних, удосконалювались не менш інтенсивно, ніж заходи захисту від них. В даний час для забезпечення захисту інформації потрібна не просто розробка окремих механізмів захисту, а реалізація системного підходу, що включає комплекс взаємопов'язаних заходів та засобів (спеціальних, технічних, програмних, організаційних, нормативно-правових, морально-етичних тощо). Комплексний характер захисту випливає з комплексних дій зловмисників, які прагнуть будь-якими засобами (заходами) добути важливу для них інформацію.

Сьогодні можна стверджувати, що захист інформації в автоматизованих системах обробки та передачі даних є питанням актуальним і потребує детального дослідження, а це вимагає значних витрат, що збільшуються, і зусиль. Проте все це дозволяє уникнути значно перевершуючих втрат і збитків, які можуть виникнути при реальному здійсненні загроз автоматизованій системі обробки та передачі даних.

Системний підхід до захисту інформації вимагає необхідність обліку всіх взаємопов’язаних, взаємодіючих і таких, що змінюються в часі елементів, умов і чинників, істотно значущих для розуміння і вирішення проблеми забезпечення безпеки автоматизованої системи обробки та передачі даних. При створенні системи захисту інформації необхідно враховувати всі слабкі, найбільш вразливі місця автоматизованої системи обробки та передачі даних, а також характер, можливі об'єкти і напрями атак на систему з боку порушників, шляхи проникнення в системи і несанкціонованого доступу до інформації. Система захисту інформації повинна будуватися з обліком не тільки всіх відомих каналів витоку інформації і несанкціонованого доступу до інформації, але і з урахуванням

можливості появи принципово нових шляхів реалізації загроз безпеці інформації.

На даний час існує широкий спектр заходів, методів і засобів захисту інформації. Їх комплексне використання припускає узгоджене застосування різнорідних засобів при побудові цілісної СЗІ, що перекриває всі існуючі канали реалізації загроз і що не містить слабких місць. Захист інформації повинен будуватися ешелоновано та ґрунтуватися на основних принципах, а саме системності та комплексності. Головну роль в СЗІ відіграють засоби захисту, які реалізовані на рівні операційної системи (ОС) внаслідок того, що ОС - це якраз та частина автоматизованої системи обробки та передачі даних, яка управляє використанням всіх її ресурсів [2].

Захист інформації - це не разовий захід і навіть не сукупність проведених заходів і встановлених засобів захисту, а безперервний цілеспрямований процес, що вимагає вживання відповідних заходів на всіх етапах життєвого циклу автоматизованої системи обробки та передачі даних, починаючи з ранніх стадій проектування, а не тільки на етапі її експлуатації. Розробка системи захисту інформації повинна вестися паралельно з розробкою системи, яка сама захищається. Це дозволить врахувати вимоги безпеки при проектуванні архітектури і створити ефективніші (як за витратами ресурсів, так і по стійкості) захищені системи. Для більшості фізичних і технічних засобів захисту для ефективного виконання їх функцій необхідна постійна організаційна (адміністративна) підтримка (своєчасна зміна і забезпечення зберігання і застосування імен, паролів, ключів шифрування, перевизначення повноважень тощо). Перерви в роботі засобів захисту інформації можуть бути використані зловмисниками для аналізу методів і засобів захисту, які вживаються, й впровадження спеціальних програмних і апаратних “закладок” і інших засобів подолання системи захисту інформації, після відновлення її функціонування.

Створити абсолютно незламну СЗІ принципово неможливо. При достатній кількості часу і засобів можливо подолати будь-який захист. Тому має сенс вести мову тільки про деякий прийнятний (достатній) рівень безпеки. Високоефективна СЗІ коштує дорого, використовує при роботі істотну частину потужності й ресурсів автоматизованої системи обробки та передачі даних і може створювати відчутні додаткові незручності користувачам. Важливо правильно вибрати той достатній рівень захисту, при якому витрати, ризик і розмір можливого збитку були б прийнятними (завдання аналізу ризику).

У якості орієнтира для оцінки достатнього рівня захисту необхідно визначити співвідношення між важливістю інформації, що захищається, і витратами на її захист. Рівень захисту раціональний, коли забезпечується необхідний рівень безпеки інформації й мінімізуються витрати на її захист, які складаються з витрат на захист інформації та збитку за рахунок перехоплення інформації противником [3].

Між цими показниками існує досить складний зв'язок, так як збиток через недостатню безпеку інформації зменшується зі збільшенням витрат на її захист.

При проектуванні АСОПІ її система захисту 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, так як навіть вимоги 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 [5].

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 і які забезпечують отримання статистичних даних [6].

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.

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 [7].

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. У міру 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.

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

Структуризація заснована на ряді положень. Інтегральний показник ефективності захисту інформації в АСОПІ 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 комплексної СЗІ, 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 [8].

Часто доводиться створювати систему захисту інформації в умовах великої невизначеності. Тому прийняті заходи і встановлені засоби захисту, особливо в початковий період їх експлуатації, можуть забезпечувати як надмірний, так і недостатній рівень захисту. Природно, що для забезпечення можливості варіювання рівнів захищеності, засоби захисту повинні володіти певною гнучкістю. Особливо важливим ця властивість є в тих випадках, коли встановлення засобів захисту необхідно здійснювати на працюючу систему, не порушуючи процесу її нормального функціонування. Крім того, зовнішні умови і вимоги з часом змінюються. У таких ситуаціях властивість гнучкості позбавить власників автоматизованої системи обробки та передачі даних від необхідності вживання кардинальних заходів щодо повної заміни засобів захисту на нові.

Сутність принципу відвертості алгоритмів і механізмів захисту полягає в тому, що захист не повинен забезпечуватися тільки за рахунок таємності структурної організації і алгоритмів функціонування її підсистем. Знання алгоритмів роботи СЗІ не повинно давати можливості її подолання, проте це зовсім не означає, що інформація про конкретну СЗІ повинна бути загальнодоступна.

Механізми захисту повинні бути інтуїтивно зрозумілі і прості у використанні. Застосування засобів захисту не повинно бути пов'язано із знанням спеціальних мов або з виконанням дій, що вимагають значних додаткових витрат при звичайній роботі законних користувачів, а також не повинно вимагати від користувача виконання рутинних малозрозумілих йому операцій. Можна настільки посилити заходи захисту інформації, що поряд зі збільшенням рівня її безпеки погіршаться умови виконання користувачами своїх функціональних обов'язків.

Таким чином варто відзначити, що неможливо охопити весь спектр питань, що виникають при розгляді проблеми захисту інформації в автоматизованій системі обробки та передачі даних, і весь спектр відповідей на них, знайдених на сьогоднішній день. Жодна, найдосконаліша система захисту інформації, зі всілякими комплексними рішеннями, не може дати стовідсоткової гарантії на безпеку даних. Адже люди, що розробили СЗІ, знають всі

слабкі місця в ній. Як показує досвід, що б не зробила людина, в цьому завжди знайдуться слабкі сторони, адже все передбачити не можливо. Проблем забезпечення технічної безпеки ще дуже багато, але ризик можна звести до мінімуму, використовуючи вищевказані комплексні підходи до захисту інформації в автоматизованих системах обробки та передачі даних.

В подальшому для захисту інформації на основі системного підходу й аналізу необхідно, поряд з організаційним і технічним, мати методичне забезпечення. Відповідно до алгоритму проектування системи захисту інформації необхідна модель, що забезпечує можливість визначення ступеня викриття циркулюючої в системі інформації, яка ґрунтується на формуванні комплексу можливих каналів витоку інформації та показників, на основі яких оцінюється можливість перехоплення та розпізнавання інформації.

ЛІТЕРАТУРА

1. Інформаційні технології управління: навч. посіб. / під ред. Ю.М. Черкасова. - М.: ІНФРА-М, 2001. – 216 с.
2. Козирев А.А. Інформаційні технології в економіці і управлінні: підручник / А.А. Козирев. - Спб.: Вид-во Міхайлова Ст. А., 2000. - 360 с.
3. Гулак Ю.С. Системний підхід до захисту інформації, яка циркулює в системі управління військами (силами) / Ю.С. Гулак // Труди університету. – 2011. – № 5 (104). – С. 89 – 94.
4. Закон України «Про захист інформації в автоматизованих системах».
5. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу // НД ТЗІ 2.5-004-99.
6. Захист інформації. Технічний захист інформації. Основні положення // ДСТУ 3396.0-96. – К.: Держспоживстандарт України, 1997. – 18 с.
7. Толюпа С.В. Комплексний підхід оцінки ефективності систем захисту інформації в інфокомунікаційних мережах нового покоління / С.В. Толюпа, О.М. Власов // Наукові записки УНДІЗ. - 2011. - №3(19), - С. 10-14.
8. Подиновский В.В. Количественная важность критериев / В.В. Подиновский // Автоматика и телемеханика. - 2000. - № 5. - С. 110-123.

Надійшла: 10.01.2013

Рецензент: д.т.н., проф. Дівізінюк М.М.