УДК 004.056
DOI: 10.31673/2409-7292.2019.015963
О.А. Лаптєв, В.І. Степаненко, Ю.О.Тихонов
http://orcid.org/0000-0002-4194-402X

ФОРМАЛЬНІ МАТЕМАТИЧНІ МОДЕЛІ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ

В даній статті обгрунтовані положення про необхідність створення оптимального підходу побудові математичної моделі безпеки, досліджені формальні математичні моделі для забезпечення безпеки інформації, огляд приведених типів формальних моделей доводить, що розробка математичних моделей формалізації процесів забезпечення безпеки інформації є складною науковою проблемою, актуальність якої лише підвищується в міру розвитку математичних методів управління і підвищення ступеня автоматизації вирішення цільових завдань безпеки інформації.
Ключові слова:математична модель,безпека інформації, математичні методи управління.

Постанова завдання.

Сучасний світ характеризується такою цікавою тенденцією, як постійне підвищення ролі інформації. Як відомо, всі виробничі процеси мають в своєму складі матеріальну і нематеріальну складові. Перша - це необхідна для виробництва обладнання, матеріали та енергія в потрібній формі (тобто, чим і з чого виготовляється предмет). Друга складова - технологія виробництва (тобто, як він виготовляється). Згадавши в загальних рисах історію розвитку продуктивних сил на Землі, кожен бачить, що роль (і, відповідно, вартість) інформаційної компоненти в будь-якому виробництві з плином часу зростає.

В останнє сторіччя з'явилося багато таких галузей виробництва, які майже на 100% складаються з однієї інформації, наприклад, дизайн, створення програмного забезпечення, реклама та інші.

Настільки ж яскраво демонструє підвищення ролі інформації в виробничих процесах поява в XX столітті такого заняття, як промислове шпигунство. Чи не матеріальні цінності, а чиста інформація стає об'єктом викрадення.

З підвищенням значущості і цінності інформації відповідно зростає і важливість її захисту.

З одного боку, інформація коштує грошей. Значить витік або втрата інформації спричинить матеріальний збиток. З іншого боку, інформація - це управління. Несанкціоноване втручання в управління може привести до катастрофічних наслідків в об'єкті управління - виробництві, транспорті, військовій справі. Функціонування підприємства неможливо без Системи Управління та Обліку (далі СУО), що забезпечує реалізацію технологічних процесів автоматизованого управління складними процесами в розподіленої системі, з урахуванням можливості порушення цих процессів як внутрішніми, так і зовнішніми дестабілізуючими факторами. Порушення процесів можливо при цілеспрямованій дії порушника на елементи СУО з метою спотворення або знищення циркулюючої інформації, а також у разі зміни технологічних циклів управління при розкритті порушником конфіденційної інформації, що привело до необхідності вжиття термінових заходів по компенсації можливих збитків. Отже, безпосереднє виконання цільових функцій СУО в часі пов'язане з об'єктивною необхідністю оперативної оцінки стану СУО в цілому, розподілу і перерозподілу ресурсів системи забезпечення безпеки інформації (далі СЗБІ), яка вирішує завдання захисту інформації в процесі функціонування СУО.

У загальному випадку СЗБІ включає в себе організаційні, технічні та програмні засоби захисту.

Організаційні засоби захисту являють собою спеціальні організаційно-технічні та організаційно-правові заходи, акти та правила, які здійснюються в процесі створення і експлуатації СУО. Даний клас засобів захисту хоч і спрямований на деякий упорядкування процесу функціонування СУО, однак практично не піддається формалізації через безпосередньої участі більшої кількості людей в їх застосуванні. Що ж стосується

функціонування технічних і програмних засобів захисту, то їх роботу можна представити у вигляді формальної моделі, яка називається моделлю забезпечення безпеки.

Необхідно зауважити, що доцільність розробки математичних моделей формалізації процесів захисту інформації не завжди очевидна. Однак існуючі складнощі та суперечності, які виникають при обґрунтуванні, створенні та застосуванні СЗБІ в складі функціонування підприємства, підтверджують актуальність проблеми розробки математичних моделей даного класу і необхідність створення для вирішення цієї проблеми відповідного методичного забезпечення.

Виклад основного матеріалу.

Відповідно до постанови Кабінету Міністрів України «Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах» від 16 листопада 2002 р. № 1772.Необхідною складовою інформаційної безпеки є захист інформації від її втрати, витоку або розголошення. Зазвичай зловмисників цікавить передусім виробничо-технологічна інформація (методи виготовлення продукції, програмне забезпечення, виробничі показники, хімічні формули, рецептури, результати випробувань дослідних зразків, дані контролю якості тощо) та ділова (результати дослідження ринку, списки клієнтів, економічні прогнози, стратегія дій на ринку тощо). Іноземні спецслужби може цікавити також стратегічно важлива для України інформація. Відповідно до інтересів забезпечення національної безпеки і ступеня цінності для держави, а також правових, економічних та інших інтересів користувачів, за режимом доступу інформація поділяється на відкриту інформацію, тобто загальнодоступну, яка використовується в роботі без спеціального дозволу, поширюється через засоби масової інформації, оголошується на конференціях, у виступах та інтерв'ю; та інформацію з обмеженим доступом, яка містить відомості, що становлять той чи той вид таємниці і підлягають захисту як з боку держави, так і відповідних користувачів. Для оцінки безпеки інформації розробляються математичні моделі формалізації процесів захисту інформації.

Під моделлю безпеки розуміється математично точний опис механізмів процедур реалізації функцій захисту інформації в усіх режимах роботи системи життєдіяльності підприємств.

По-перше, знову створювана СУО вимагає техніко-економічного обґрунтування всіх сторін функціонування, в тому числі і принципів забезпечення безпеки інформації. При цьому обґрунтування має ґрунтуватися на розробці і дослідженні математичних моделей забезпечення безпеки, а результати цих досліджень повинні бути доказом безпеки інформації в реальній системі при точному дотриманні всіх принципів захисту, закладених у формальній моделі. Однак протиріччя полягає в тому, що цілеспрямоване дослідження моделі може бути проведено лише за умови повної інформації про функціонування СУО в цілому, що можливо далеко не завжди, особливо для складних розподілених систем. У деяких випадках використовується інформація про функціонування окремих елементів або підсистем СУО, а на її основі робляться висновки про всю систему в цілому. Отже, необхідно створювати моделі забезпечення безпеки для окремих процесів в СУО та методи їх інтеграції, що забезпечують безумовне виконання всіх вимог щодо захисту інформації.

По-друге, на розробку СУО завжди виділяються кінцеві ресурси, які розробник розподіляє на всі технологічні етапи - від обґрунтування вигляду майбутньої СУ до проведення випробувань її компонентів і впровадження. Даний фактор породжує протиріччя, пов'язане з бажанням розробника мінімізувати витрати на попередні модельні дослідження при явної необхідності виявлення на ранніх етапах проектування всіх можливих каналів витоку. Відбувається суб'єктивне протиставлення необхідності проведення модельних досліджень розробці об'єктів реальної системи. В цьому випадку система створюється без попереднього вивчення всього комплексу протікають в ній процесів при їх взаємозв'язку з технологічними особливостями захисту інформації. У граничному випадку

ігнорування попередніх досліджень на моделях може призвести до повної незахищеності системи навіть при включенні до складу програмно-апаратних засобів СУО великого числа дорогих і ресурсномістких засобів захисту. Отже, формалізація процесів забезпечення безпеки інформації не повинна бути для розробника складною і трудомісткою завданням, що можливо лише при наявності науково обґрунтованих типових моделей і добре відпрацьованого методичного забезпечення їх застосування.

По-третє, технічні та програмні засоби, що утворюють СЗБІ і за допомогою яких в СУО вирішуються завдання захисту інформації, вимагають резервування певної частини ресурсів СУО. Наприклад, управління процесами захисту вимагає наявності спеціальної служби, розсилка ключової інформації - додаткової пропускної здатності каналів зв'язку, контроль доступу до ресурсів - витрат часу і т.п . У цьому випадку виникає протиріччя між завданнями СУО як системи, максимально поліпшує характеристики процесів управління за рахунок повнішого використання власних ресурсів, і завданнями СЗБІ, що використовує ресурси СУО для досягнення цілей, які не завжди збігаються з головними цілями СУО. Це протиріччя посилюється тим, що незважаючи на технічну і технологічну можливість суміщення рішення деяких завдань в рамках обчислювальних засобів одного об'єкта СУО, з точки зору захисту інформації таке поєднання просто неприпустимо внаслідок різного призначення і різних грифів секретності оброблюваної інформації. Отже, виникає завдання планування завантаження ресурсів СУО для їх оптимального використання з урахуванням вимог безпеки інформації, що можливо лише на основі формальної моделі забезпечення безпеки.

По-четверте, досягнення необхідних значень показників безпеки інформації в розподіленої СУО з динамічно змінюваними інформаційно-логічними зв'язками можливо лише в разі організації єдиного керування всіма ресурсами системи захисту, причому в будь-який момент часу повинна забезпечуватися можливість:

- проведення аналізу стану засобів захисту і СЗБІ в цілому;
- прогнозування поведінки СЗБІ, визначення і контролю виконання умов переходу в новий стан;
- планування процесів захисту з урахуванням можливих спроб несанкціонованого доступу до інформації, в тому числі і успішно реалізованих;
- формування інформації для необхідних управляючих впливів в разі необхідності коригування процесів захисту.

Протиріччя полягає в тому, що подібне функціонування СЗБІ неможливо без "вбудованої" в систему її власної моделі, яка має властивість ізоморфізму. Однак простого ізоморфізму недостатньо. Модель системи захисту повинна об'єднуватися з моделлю зовнішнього середовища, т.е. СУО в цілому, а також з моделлю порушника. Цілком очевидно, що моделі цього типу для своєї реалізації потребують ресурси, які можна порівняти з ресурсами, необхідними для реалізації завдань СУО. Отже, необхідна розробка не тільки самих моделей формалізації процесів захисту, але і методичних основ оптимізації моделей і їх компонентів, синтезу моделей з наявних складових.

Існуючі технології формального опису процесів забезпечення безпеки інформації ґрунтуються на поняттях теорії кінцевих автоматів, теорії множин, теорії графів, тимчасової і математичної логіки, І алгебраїчних специфікацій. При цьому застосовується для опису моделі математичний апарат вносить деякі обмеження на ступінь деталізації процесів захисту, що зумовлено відмінностями фізичної сутності описуваних за допомогою використовуваних понять процесів. Наприклад, моделі, засновані на теорії множин, з більшою детальністю описують процеси контролю доступу до ресурсів системи, так як мають розвинений апарат визначення взаємовідносин між множинами об'єктів-ресурсів і об'єктів-користувачів. У той же час моделі, засновані на теорії графів, дозволяють більш глибоко визначити процеси захищеної передачі даних.

Ґрунтуючись на аналізі принципів опису процесів захисту даних і використовується при цьому математичного апарату, можна виділити наступні чотири класи формальних моделей безпеки:

- моделі трансформації станів кінцевого автомата;
- моделі запозичення і передачі повноважень;
- семантичні моделі;
- моделі інформаційних потоків.

Необхідно зауважити, що в даний час число публікацій, в яких описуються моделі безпеки, безперервно зростає. Тому в подальшому посилання наводяться тільки на ті роботи, в яких описані моделі з явно вираженими відмітними ознаками. [1]

Моделі трансформації стану є найбільш загальними і засновані на описі системи у вигляді кінцевого автомата. Моделі цього класу дозволяють найбільш повно описати процеси захисту інформації та їх взаємозв'язок з технологією обробки інформації в СУО. В якості основи більшість моделей трансформації станів використовують модель Белла-Лападули.

Модель Белла - Лападули є моделлю розмежування доступу до інформації, що захищається. Вона описується кінцевим автоматом з допустимим набором станів, в яких може перебувати інформаційна система. Всі елементи, що входять до складу інформаційної системи, розділені на дві категорії - суб'єкти і об'єкти. Кожному суб'єкту присвоюється свій рівень доступу, відповідний ступеня конфіденційності. Аналогічно, об'єкту присвоюється рівень секретності. Поняття захищеної системи визначається наступним чином: кожне стан системи повинно відповідати політиці безпеки, встановленої для даної інформаційної системи. Перехід між станами описується функціями переходу. Система знаходиться в безпечному стані в тому випадку, якщо у кожного суб'єкта є доступ тільки до тих об'єктів, до яких дозволений доступ на основі поточної політики безпеки. Для визначення, чи має суб'єкт права на отримання певного виду доступу до об'єкта, рівень секретності суб'єкта порівнюється з рівнем секретності об'єкта, і на основі цього порівняння вирішується питання, надати чи ні запитуваний доступ. Набори рівень доступу / рівень секретності описуються за допомогою матриці доступу[1].

Моделі запозичення і передачі повноважень в основному формулюються в поняттях теорії множин або теорії графів. В основі всіх моделей цього класу в явному або неявному вигляді лежить матриця контролю доступу, що є істотним обмеженням при описі динамічних операцій присвоєння або зміни класифікації ресурсів системи.

Семантичні моделі використовують поняття теорії множин і теорії предикатів і визначають правила розмежування доступу до ресурсів системи у вигляді тверджень, які можуть змінюватися в процесі виконання операцій моделі за допомогою спеціальної системи команд.

Семантична модель інформаційної безпеки - інформаційна модель має в загальному вигляді вигляд орієнтованого графа, вершини якого відповідають об'єктам предметної області-інформації, а дуги (ребра) задають відносини між ними. Об'єктами можуть бути поняття, події, властивості, процеси [2]. Таким чином, семантична мережа відображає семантику предметної області у вигляді понять і відносин.

Моделі інформаційного потоку ґрунтуються на решітці безпеки Фентона і визначають порядок взаємодії об'єктів системи в термінах перенесення інформації. Поява моделей даного класу супроводжувалося досить цікавими і перспективними теоретичними дослідженнями, проте в подальшому було показано, що моделі інформаційного потоку можуть бути описані в термінах трансформації станів об'єктів, які отримують або віддають інформацію з відповідними цифрами.

Варіантом моделі управління доступом є модель інформаційних потоків (Denning, 1983), яка призначена для аналізу потоків інформації з одного об'єкта в інший на підставі їх міток безпеки

Безпека інформаційних потоків - набір вимог і правил, спрямованих на визначення того, які інформаційні потоки в системі є дозволеними, а які ні. Дана модель не є самостійною, і використовується на додаток до мандатної або дискреційної моделі управління доступу.

На підставі проведеного аналізу формальних моделей безпеки очевидно проблеми безпеки ототожнюються з проблемою надійності і очевидно необхідно застосувати математичний апарат, який використовується в теорії надійності, де широко використовується апарат теорії ймовірності та математичної статистики. Поняття надійності і безпеки близькі, тому, основним математичним підходом до дослідження безпеки повинен стати «ймовірносно-статистичний підхід», і що «застосування формальних методів до опису безпечно ти також дозволить більш чітко визначити зв'язок між поняттями безпеки і надійності ». [3]

Однак ймовірносно-статистичний підхід на практиці застосовується досить рідко і в специфічних випадках. Його, як правило, застосовують для підтвердження правильності висновків, зроблених на підставі експертних оцінок, але не для того, щоб на підставі проведених розрахунків робити такі висновки. Це обумовлено, перш за все, тим, що для отримання достовірного результату необхідні достовірні вихідні дані. А їх в сфері безпеки і, особливо в сфері безпеки об'єктів інформатизації, в Україні немає. По-перше, тому що не створений механізм збору такої інформації, а, по-друге, тому що потерпілі досить часто приховують інформацію про інциденти що відбулися у них, щоб не зазнати ще й репутаційні витрати. Якщо і здійснюється окремими компаніями діяльність зі збору та аналізу статистичних даних, то робиться це на підставі закордонного досвіду.

Висновки.

1. Досліджені формальні математичні моделі забеспечення безпеки інформації. Ці дослідження доводять, що розробка математичних моделей формалізації процесів забезпечення безпеки інформації в СУО є складною науковою проблемою, актуальність якої лише підвищується в міру розвитку і впровадження в СУО математичних методів управління і підвищення ступеня автоматизації вирішення цільових завдань.

2. На основі сформульованих положень та приведеного аналізу запропонован ймовірносно-статистичний підхід побудові математичної моделі безпеки, який дозволяє найбільш повно оцінювати процес забезпечення безпеки інформації який також застосовують для підтвердження правильності висновків при застосуванні різних типів моделей.

Список використаних джерел

1.Методы и средства инженерно-технической защиты информации / [В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, Т.Р Гайнулин]// Litres.- 2015-С.147-148.

2.Википедия [Електронний ресурс] // Режим доступу https://ru.wikipedia.org/wiki. Html (7.05.2019)

3. Анализ математического апарат и методов ,применяемых для оценки безопасности объектов информатизации. Атаманов Геннадий, [Електронний ресурс] // Режим доступу https://bis-expert.ru/blog/4042/58272 (07.05.2019).