Наприклад, кількість квадратів четвертого порядку $K(4)=576$, а восьмого - $K(8)=10877603245908295680 0 \approx 10^{20}$.

На перетворення надходять блоки даних у тому порядку, який надає етап зчитування, і блоки гами (псевдовипадкові числа, що формуються залежно від секретного ключа). Нехай послідовність блоків даних, що підлягають перетворенню, має вигляд **M**={ m_1, m_2,…, m_n}, а послідовність блоків гами - **G**={ g_1, g_2,…, g_n}. Результат перетворення при зашифруванні **C**={ c_1, c_2,…, c_n} визначається як значення функції $c_i = L_j(m_i, g_i)$, де j - номер використовуваного латинського квадрату, що формується псевдовипадковим чином залежно від секретного ключа. Результат перетворення при розшифруванні визначається як значення функції $m_i = \overline{L}_j(c_i, g_i)$, де $\overline{L}_j$ означає латинський квадрат, що описує перетворення, обернене до перетворення латинським квадратом L_j.

Секретний ключ має складові, що визначають правила зчитування і записування блоків даних, генерування гами та вибору латинських квадратів із заданого їх набору.

УДК 004.94.355

МЕРЕЖЕВО-ЦЕНТРИЧНА ПАРАДИГМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В АВТОМАТИЗОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ УПРАВЛІННЯ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

В.О. Крайнов

Національний університет оборони України імені Івана Черняховського

Процес впровадження автоматизованих інформаційних систем у військову справу спрямований на підвищення ефективності роботи органів військового управління. Однією з найважливіших функцій у діяльності органів управління є вироблення пропозицій для прийняття обґрунтованого рішення командиром. Основою для виконання цієї функції є інформація про свої війська, війська противника, умови ведення бойових дій та ін. Перш ніж інформацію можна було б використовувати, її необхідно зібрати, систематизувати, обробити і тільки після цього в потрібному вигляді видати користувачу. Для вирішення цих задач у штабах створюються автоматизовані інформаційні системи (АІС). Слід зауважити, що будь-яка АІС для надійного функціонування має бути забезпечена надійною системою інформаційної безпеки.

Проте наявність уразливостей та кіберзагроз породжує кіберінциденти, для локалізації та нейтралізації яких необхідні ефективні методи виявлення, ідентифікації, оброблення та розслідування. Одним із підходів є застосування мережево-центричної парадигми інформаційної безпеки, яка орієнтована на протидію виникненню та ліквідації наслідків кіберінцидентів за допомогою засобів, об’єднаних інформаційними мережами в єдину систему. З огляду на динаміку

розвитку комп'ютерних технологій, пов'язаних з "мережево-центричною" обробкою даних. Маніпуляція і обмін складними даними відбувається в масштабах усе більших і складних неоднорідних мереж, що спонтанно поширюються в неконтролюємому просторі Інтернет. Нова, мережево-центрична (network centric) парадигма інформаційної безпеки, як концептуальна схема (модель) постановки й вирішення проблеми, випливає насамперед з підвищених вимог до живучості АІС, які характеризуються високим ступенем розподілу ресурсів (обслуговуванням, логікою, програмним й апаратним забезпеченням, телекомунікаціями) і практично повною відсутністю централізованого керування. Концептуальна модель ешелонованої багатошарової системи інформаційної безпеки яка зараз використовується у США, містить у собі набір компонентів, що реалізують функції моніторингу, захисту й адаптації інформаційних ресурсів, які в сукупності дозволяють поетапно запобігти проникненню, виявити факт порушення, локалізувати об'єкт впливу, нейтралізувати й видворити порушника, відновити втрачені функції системи (рис.1). В основі даної моделі системи інформаційної безпеки лежить широке використання пасивних (фільтрів, екранів) і активних (датчиків виявлення вторгнення, розпізнавання аномального поводження, адаптивних алгоритмів відновлення)технічних засобів захисту. Американський досвід використання технології IDS (Intrusion Detection Systems) у різних галузях говорить про те, що не дивлячись на очевидні

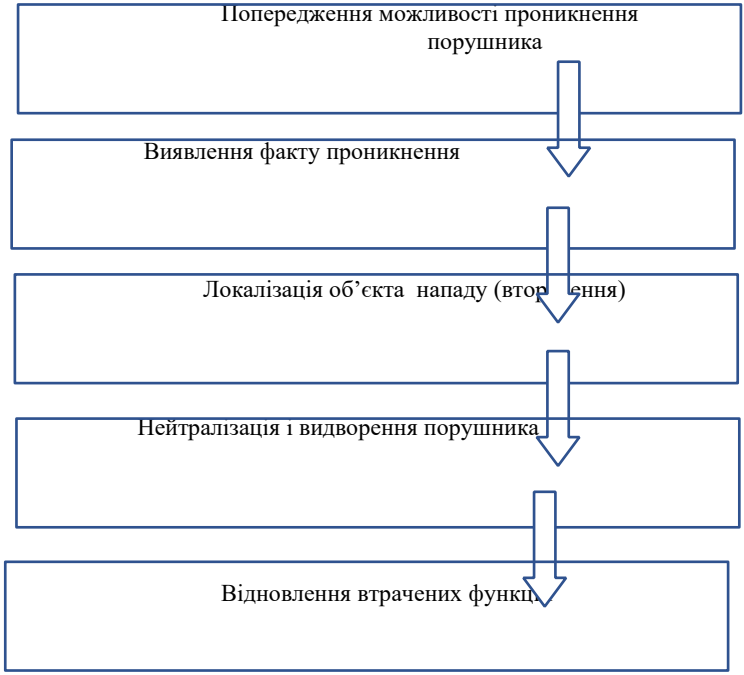

Рис. 1. Концепція ешелонованої системи захисту інформаційних ресурсів

переваги цього напрямку інформаційної безпеки (автономність, гнучкість, адресність, оперативність й ін.) його розповсюдження пов'язане із цілим рядом проблем, як об'єктивного, так і суб'єктивного походження, серед яких можна виділити в якості превалюючих відомчі інтереси й (authentication, non repudiation) і забезпечення надійності (availability) функціонування системи. Закордонний й вітчизняний досвід показує, що це завдання найбільш ефективно вирішується за допомогою методів криптографії в сполученні з використанням перевіреного та ліцензованого програмного забезпечення, а також надійними інтелектуальними носіями ключової інформації (матеріалу ключа)організаційно-технічні експлуатації. У цілому забезпечення інформаційної безпеки сьогодні містить у собі такі поняття як цілісність (integrity) інформації, конфіденційність (confidentiality) і захищеність від несанкціонованого доступу. Забезпечення цілісності інформації й автентичності (особистості) користувача в даний час найбільш ефективно реалізується за рахунок використання електронного підпису на основі несиметричних криптографічних алгоритмів із двома ключами (особистим і загальним) у поєднанні із системою посвідчувальних центрів. У США цей концептуальний підхід до захисту інформаційних ресурсів отримав назву "інформаційної гарантії" (information assurance)який суттєво розширив рамки класичного поняття інформаційної безпеки (INFOSEC). Фактично концепція інформаційної гарантії в США розглядається як оборонна інформаційна операція, в ході якої також при випадковому або навмисному викривленні інформації, несанкціонованому проникненню або навмисному вторгненні в контур управління, втрати частини ресурсів і перевантаження трафіку комплекс організаційно-технічних заходів захисту повинен забезпечити виконання найбільш важливих завдань. Іншими словами, не тільки відмови та збої устаткування, перекручування й витік інформації, але й терористичні акти на об'єктах інформаційної інфраструктури розглядаються вже не як потенційні загрози, а як системотехнічні фактори зовнішнього середовища з усіма випливаючими наслідками.

Таким чином, концепція інформаційної безпеки 21-го століття випливає перш за все із підвищених вимог до живучості інформаційних систем що виходять за рамки підприємств, відомств ті кордонів держав, які характеризуються високим ступенем розподілу ресурсів і практично повною відсутністю централізованого управління. Системи інформаційної безпеки майбутнього повинні не тільки й не стільки обмежувати допуск користувачів до програм і даних, скільки визначати і делегувати їхні повноваження в корпоративному вирішенні завдань, виявляти аномальне використання ресурсів, прогнозувати аварійні ситуації й усувати їхні наслідки, гнучко адаптуючи структури в умовах відмов, часткової втрати або тривалого блокування ресурсів.