УДК 681.3

О.С. Петров,
О.П. Український

КЛЮЧОВІ ПОНЯТТЯ ФУНКЦІОНУВАННЯ СИСТЕМИ ПРОТИДІЇ ВНУТРІШНЬОМУ ВИТОКУ ІНФОРМАЦІЇ

У статті розглянуто ключові визначення та алгоритми системи протидії внутрішньому витоку інформації.

Ключові слова: *витік інформації, обсяг інформації, протидія внутрішньому витоку інформації.*

В статье рассмотрены ключевые определения и алгоритмы системы противодействия внутренней утечке информации.

Ключевые слова: *утечка информации, объем информации, противодействие внутренней утечке информации.*

Key definitions and algorithms of the system of counteraction of internal information leakage are considered.

Keywords: *information leakage, body of information, counteraction of internal information leakage.*

Основною метою будь-якої системи інформаційного захисту є створення умов для запобігання чи унеможливлення несанкціонованих дій з інформацією, що знаходиться всередині цієї системи. Для цього реалізують два напрями комплексних заходів: пасивні та активні.

Для дієвої системи інформаційного захисту головну роль відіграють активні заходи захисту інформації. Саме на них має базуватися майбутня модель інформаційної безпеки.

Розглянемо ключові поняття, що будуть використовуватися при розгляді математичної моделі запобігання внутрішньому витоку інформації.

Внутрішній витік інформації є окремим випадком порушення цілісності безпеки інформаційної системи. Саме тому алгоритм протидії порушенню цілісності безпеки інформаційної системи [1] можна використати як основу та адаптувати для протидії внутрішньому витоку інформації.

Протидія внутрішньому витоку інформації це така дія інформаційної системи, яка базується на таких засадах:

1) створення сигналів попередження про спроби несанкціонованого доступу;

2) обмеження чи блокування зони витоку;

3) відмова в подальших діях у зоні витоку.

Протидія можлива на базі прийняття рішень оператором системи, в напівавтоматичному та автоматичному режимі.

Метою протидії внутрішньому витоку інформації є:

1) зменшити до мінімуму або зовсім уникнути можливості несанкціонованого витоку будь-якого обсягу інформації з інформаційної системи;

2) зменшити до мінімуму час несанкціонованого витоку інформації з інформаційної системи;

3) дезорганізувати спроби несанкціонованого витоку інформації;

4) диференціювати джерело та суб'єкт несанкціонованого витоку інформації.

Під *обсягом інформації* будемо розуміти ту кількість інформації, яку було виведено за інформаційну систему, або змінено, пошкоджено чи знищено в рамках інформаційної системи суб'єктом інформаційної діяльності, що не мав на це санкціонованого права.

Під *часом несанкціонованого витоку інформації* будемо розуміти той час, який пройшов з моменту початку несанкціонованого витоку інформації до моменту, коли такий витік було виявлено.

Під *дезорганізацією спроби несанкціонованого витоку інформації* будемо розуміти таку реакцію системи, що приведе до блокування дій суб'єкта несанкціонованого доступу.

Під *диференціюванням суб'єкта несанкціонованого витоку інформації* будемо розуміти його однозначну аутентифікацію.

Під *диференціюванням джерела несанкціонованого витоку інформації* будемо розуміти однозначну аутентифікацію моделі несанкціонованого витоку інформації.

Для реалізації цих пунктів мети потрібно, щоб система запобігання внутрішньому витоку інформації мала можливість коректно (коректно з огляду на протидію негативним наслідкам витоку) приймати рішення. А для цього потрібно описати математичну модель, на базі якої буде прийматися рішення про керування системою захисту інформації.

Наведена математична модель [2], описує загальну взаємодію між чинниками від яких залежіть безпека інформації системи:

$$\sum_{i}^{n} f(C_i, I_i, A_i) \to max, \quad npuf(C_i, I_i, A_i) > D_{зад} \tag{1}$$

де $f(C_i, I_i, A_i)$ – значення функції ІБ для і-ої загрози; п – кількість загроз; C_i, I_i, A_i – ймовірність порушення цілісності, доступності та конфіденційності для і-ої загрози; $D_{зад}$ – заданий рівень ІБ для і-ої загрози.

Якщо ввести додатковий параметр часу, формула матиме такий вигляд:

$$\sum_{i}^{n} f(C(\Delta t)_i, I(\Delta t)_i, A(\Delta t)_i) \to max, \quad при \Delta p > t_{зад}; \Delta t = t_{ку} - t_{ну} \tag{2},$$

де Δt – час протягом якого реалізується і-я загроза цілісності, доступності або конфіденційності ІБ; $t_{зад}$ – час протягом якого необхідно підтримувати заданий рівень ІБ. Один з методів кількісного оцінювання виразів (1) і (2) пропонується автором цієї моделі в своїй публікації [3].

Пропонується удосконалити цю модель, поширивши значення C_i, I_i, A_i критеріями безпеки, які надано в документі НД ТЗІ 2.5-004-99 [4].

На базі цієї моделі можливо зробити кількісну оцінку показника ІБС та розробити систему прийняття рішення запобігання внутрішньому витоку інформації.

Зважаючи на те, що задача прийняття рішення – це задача алгоритмізації дій у системі по недопущенню витоку інформації чи зменшенню об'єму цього витоку, то встає потреба структурувати цей алгоритм.

Університет SANS у своєму документі [5] пропонує шість головних етапів захисту інформаційної системи (рис. 1):

1. Preparation (підготовка). Один з найкритичніших етапів. Він складається зі встановлення головних компонентів захисту на всі вузли системи; автори документу зазначають, що всі вузли системи повинні мати хоча б мінімальний рівень захисту. Якщо цього не зробити, механізм витоку інформації може спрацювати за принципом ланцюгової реакції на кожному вузлі системи.

2. Identification (ідентифікація). На цьому етапі запускається механізм розпізнавання порушення інформаційної безпеки (витоку інформації) та відбувається підтвердження чи спростування цього витоку. Якщо підтвердження витоку було зроблено, то реалізується алгоритм формалізації цього витоку (відстежується час початку витоку, фізичне розташування вузла витоку тощо).

3. Containment (стримування). Це етап на якому система намагається локалізувати дії, що призводять до витоку інформації, та запобігти поширенню цих дій на інші вузли системи, або, якщо потрібно, на інші системи.

4. Eradication (викорінення). Якщо це можливо, на цьому етапі проводиться винищення джерела, що спричинило порушення інформаційної безпеки (витоку інформації).

5. Recovering (відновлення). Цей етап спрямований на відновлення системи до функціонального стану, який вона мала до початку порушення інформаційної безпеки.

6. Follow-up (слідування). На цьому етапі проводиться повне розслідування інциденту, щоб запобігти його повторенню у майбутньому.

Рис. 1. Алгоритм взаємодії етапів захисту інформаційної системи

Запропонована математична модель може бути адаптована до етапів ідентифікації та стримування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Оссовский С.* Нейронные сети для обработки информации / С. Оссовский ; пер. с польского И.Д. Рудинского. – М. : Финансы и статистика, 2002. – 344 с.

2. *Певнев В.Я.* Математическая модель информационной безопасности / В.Я. Певнев, М.В. Цуранов. – Харків : Системи обробки інформації, 2010. –випуск 3 (84). – 62 с.

3. *Певнев В.Я.* Эффективность информационной безопасности замкнутых систем / В.Я. Певнев // Радіоелектронні і комп'ютерні системи. – 2009. – № 5. – С. 82–85.

4. НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу" [Електронний ресурс]. – Режим доступу : http ://am-soft.ua/files/KSZI/2.5-004-99.pdf

5. *Браун Д.* Интерактивный анализ компьютерных преступлений / Д. Браун, Л. Гундерсон, М. Эванс // Открытые системы. – 2000. – № 11. – С. 40–49.

Отримано 17.06.2011