УДК 004.056
Савченко Ю. В.[1], Карпуков Л.М.[2], Воскобойник В.О.[3], Івахова Ю.В.[4]
[1] канд. техн. наук, доц. Університету митної справи та фінансів
[2] д-р техн. наукт.н., проф. НУ «Запорізька політехніка»
[3] канд. техн. наук, проф. НУ «Запорізька політехніка»
[4] студ. гр. Б21-1 Університету митної справи та фінансів

МОДЕЛЮВАННЯ ПРОЦЕСІВ НАПАДУ НА ІНФОРМАЦІЮ ТА ЇЇ ЗАХИСТУ

Кібербезпека залишається головною проблемою в сучасному IT-світі оскільки кількість хакерських інцидентів зростає. Багато аспектів нашого життя перемістилися в Інтернет, що комерційний і приватний світи можуть багато втратити через порушення безпеки.

У відповідь спеціалісти з кібербезпеки розгортають арсенал засобів захисту та протидії, щоб забезпечити безпеку транзакційних даних і конфіденційної інформації. Враховуючи величезну кількість і різноманітність доступних сьогодні атак, це величезне завдання.

Ціллю даної роботи є моделювання загроз та захисту інформації на основі аналізу процесів моделювання нападу на інформацію і доступні методології, а також існування яких моделей спрямоване на захист інформації і на основі чого ці моделі розроблені.

Модель безпеки конкретно визначає основні аспекти безпеки та їх зв'язок із продуктивністю операційної системи. Жодна організація не може захистити свою конфіденційну інформацію чи дані, не маючи ефективних і ефективних моделей безпеки. Можна сказати, що основною метою моделі безпеки є забезпечення необхідного рівня розуміння для успішної та ефективної реалізації ключових вимог захисту. Моделі інформаційної безпеки — це процедури, які використовуються для перевірки політик безпеки, оскільки вони передбачають надання точного набору вказівок, яким комп'ютер може слідувати для реалізації життєве важливих процесів безпеки, процедур і концепцій, що містяться в програмі безпеки. Ці моделі можуть бути інтуїтивно зрозумілими або абстрактними. Моделі безпеки керують напрямками безпеки операційних систем.

Існують деякі моделі безпеки, які найчастіше використовуються для пояснення вказівок і правил, які керують конфіденційністю, захистом і цілісністю інформації. Основною причиною та фокусом на реалізації моделі безпеки є конфіденційність, яка не враховує контролю доступу та цілісності інформації. За допомогою цих моделей безпеки, які є основними компонентами, на які слід звернути увагу при розробці політик і систем інформаційної безпеки. Ці моделі розповідають про правила доступу,

необхідні для створення екземпляра визначеної політики та виділення об'єктів, які керуються політикою компанії.

Ось деякі з важливих моделей, які ми обговорюємо нижче, щоб зрозуміти функції та важливість моделей інформаційної безпеки в сучасному діловому світі.

Модель Bell-LaPadula спочатку стала розробкою Міністерства оборони США (DoD). Ця модель є початково математичною моделлю багаторівневої політики безпеки, яка пояснює концепцію безпечного стану та обов'язкових методів доступу. Це гарантує, що дані передаються лише таким чином, щоб не порушувати політику системи та зосереджено на конфіденційності.

Деякі проблеми, пов'язані з реалізаціями Bell-LaPadula, пов'язані з тим, що користувачі, звичайно, не можуть спілкуватися з користувачами з низьким рівнем. З одного боку, коли модель BLP звертається до конфіденційності, вона не враховує приховані канали чи контроль доступу, з іншого боку. Крім того, будь-хто може створити об'єкт вищої класифікації, що також є проблемою. Спочатку модель Белла-ЛаПадули мала завершити потреби Міністерства оборони для InfoSec, наразі військові прагнуть і досягають цілей, практикуючи забезпечення дискретної сегрегації та контролю доступу.

Модель Clark Wilson має справу з двома видами об'єктів, один з яких ми назвали CDI та UDI, тобто елементи даних з обмеженнями та елементи даних без обмежень. Він також має два типи зв'язків: перший – IVP, що означає процедуру перевірки цілісності, а другий – TP, тобто процедура транзакції. Робота IVP полягає в тому, щоб переконатися, що TP, які спричиняють CDI, перебувають у правильному стані, і дійсні сертифікати перетворення для всіх TP. Тут лише авторизовані TP можуть контролювати CDI. Іншими словами, щоб захистити цілісність інформації та забезпечити правильно відформатовані транзакції, ця модель цілісності повинна бути добре реалізована.

Модель Biba трохи схожа на BLP, хоча вона не наголошує на конфіденційності, основна увага моделі Biba зосереджена на цілісності, і її часто використовують для цілісності, де конфіденційність важливіша. Ми можемо дивитися на це просто як на протилежну реалізацію BLP. Конфіденційність є головною проблемою багатьох урядів, але більшість підприємств хочуть забезпечити цілісність безпеки даних на найвищому рівні. Biba є зразком вибору, коли безпека цілісності життєве важлива.

Два основних правила моделі *Biba*:

Проста аксіома цілісності: (без зчитування) суб'єкт на рівні дозволу не може прочитати інформацію з нижчою класифікацією. Це допомагає особам отримати доступ до важливих даних на нижчому рівні цілісності. Це гарантує цілісність, запобігаючи впливу поганої інформації з нижчих рівнів цілісності.

Аксіома цілісності: (без запису) суб'єкт на рівні дозволу не може записати інформацію до вищої класифікації. Це допомагає суб'єктам передавати важливу інформацію до вищого рівня цілісності, ніж дозвіл на зміни. Це гарантує цілісність, запобігаючи переміщенню поганого матеріалу на вищі рівні цілісності.

Brewer and Nash модель також відома як модель «китайської стіни» і використовується для уникнення конфлікту інтересів шляхом заборони окремій особі, наприклад консультанту, входити до кількох COI, тобто категорій конфлікту інтересів. Зміна політик контролю доступу залежить від поведінки користувача. Це означає, що якщо особа, яка отримує доступ до інформації, що стосується однієї сторони, не може отримати доступ до даних іншої сторони або дані для тієї самої особи недоступні.

Модель *Harrison Ruzzo Ullman* також вважається доповненням до моделі BLP. Модель Белла-ЛаПадули не має системи для зміни привілеїв доступу або для створення та видалення суб'єктів і об'єктів. Модель вирішує ці проблеми шляхом авторизації структури для розподілу прав доступу та перевірки відповідності даній політиці, що припиняє несанкціонований доступ. Модель Harrison Ruzzo Ullman може бути реалізована за допомогою контролю доступу або списку можливостей.

Одним із найважливіших завдань у сфері інформаційної безпеки є якісна оцінка загроз. Саме достовірний результат такої оцінки є основою для раціонального вибору засобів і методів захисту інформації. Існує кілька відомих інструментів для оцінки інформаційної безпеки, моделювання заходів безпеки та можливих типів загроз інформаційній безпеці, основні з яких представлені в [1-5]. Ці моделі побудовані на основі теорії ймовірностей та математичної статистики, нечіткі множин, теорії ігор, теорії графів, теорії цифрових автоматів , мережі Петрі, теорії випадкових процесів тощо.

Ці методології утворюють набір інструментів для аналізу продуктивності досліджуваних інформаційних систем протягом обмеженого цензурованого періоду часу. Аналіз відбувається в контексті визначення: періоду час між відмовами в досліджуваній системі; кількості відмов у досліджуваній системі за цензурований період її роботи; реакції досліджуваної системи на спровоковані збої; реакції досліджуваної системи на комплексні тестові впливи.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. S. Colabianchi, F. Costantino, G. Di Gravio, F. Nonino, R. Patriarca Discussing resilience in the context of cyber physical systems Comput Ind. 2021, 10.1016/j.cie.2021.107534

2. H.S. Lallie, K. Debattista, J. Bal A review of attack graph and attack tree visual syntax in cyber security Computer Science Review. 2020, 10.1016/j.cosrev.2019.100219

3. George, P.G., Renjith, V.R., 2021. Evolution of Safety and Security Risk Assessment methodologies towards the use of Bayesian Networks in Process Industries. *Process Safety and Environmental Protection*. 10.1016/j.psep.2021.03.031

4. L. Zhang, V.L.L.Three decades of deception techniques in active cyber defense – Retrospect and outlook Computers & Security. 2021, 10.1016/j.cose.2021.102288

5. D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, N. Meskin Cybersecurity for industrial control systems: A survey Computers & Security10.1016/j.cose.2019.101677