ІНФОРМАЦІЙНА ТА КІБЕРНЕТИЧНА БЕЗПЕКА

УДК 005.8:316.422
DOI https://doi.org/10.17721/ISTS.2021.1.17-24

Н. В. Лукова-Чуйко, orcid.org/0000-0003-3224-4061,
lukova@ukr.net
С. В. Толюпа, orcid.org/0000-0002-1919-9174,
tolupa@i.ua
І. І. Пархоменко, orcid.org/0000-0001-6889-9284,
parkh08@gmail.com
Київський національний університет імені Тараса Шевченка, Київ, Україна

МЕТОДИ ВИЯВЛЕННЯ ВТОРГНЕНЬ У СУЧАСНИХ СИСТЕМАХ IDS

Нині гостро стоїть проблема захисту інформаційно-комунікаційних систем і ресурсів кібернетичного простору. Швидкий розвиток інформаційної сфери приводить і до модернізації та ускладнення методів проведення атак на об'єкти кібернетичного простору. Кожного року зростає статистика вдалих атак на комп'ютеризовані системи різних організацій, включаючи і державні установи. Із цього можна зробити висновок, що навіть найнадійніші системи захисту не дають стовідсоткової гарантії захисту. Однією з можливих причин такого стану речей може бути саме використання більшістю систем безпеки стандартних механізмів і способів захисту. До таких механізмів належать – розмежування доступу, яке базується на правах суб'єкта доступу, шифрування й ідентифікація, і аутентифікація. Традиційні способи не можуть захисти від власних користувачів, які мають злочинні наміри. Крім того, цей підхід не вирішує проблеми чіткого поділу наявних суб'єктів системи на предмет авторизованого використання глобалізованих ресурсів, можливості підбору паролів із застосуванням спеціалізованого програмного забезпечення, а також залишається проблема обмеження доступу до ресурсів інформаційної системи, що може мати як наслідок зменшення продуктивності й ускладнення проходження транзакцій між компонентами вказаної системи. Виникає потреба застосовувати механізми, які б не відкидали переваги традиційних, але і доповнювали б їх. А саме, щоб ці механізми виявляли спроби неавторизованого, несанкціонованого доступу, надавали інформацію про такі спроби, і крім того, могли реагувати у відповідь. Одним із ключових факторів використання таких систем захисту є їхня здатність запобігати атакам зловмисників, які були аутентифіковані й авторизовані з додержанням усіх процедур і правил доступу й отримали необхідні права на певні дії. Звичайно неможливо передбачити повний набір сценаріїв подій у системі з авторизованим користувачем, який має зловмисні наміри, але необхідно зробити детальний опис можливих "зловмисних" сценаріїв, або піти від зворотного й описати так звані "нормальні" сценарії. Опис "нормальних сценаріїв" дасть можливість виявити небезпечну активність, адже ця активність буде мати відхилення від так званого "нормального" сценарію поведінки в системі навіть авторизованим користувачем. Отже дослідження можливостей використання механізмів, які спрямовані на виявлення аномалій у системі або на пошук зловживань, можуть допомогти реалізувати ефективні рішення для систем виявлення та попередження вторгнень.

Ключові слова: *система виявлення вторгнень, виявлення статистичних аномалій, виявлення на основі сигнатур, безпека інформаційних технологій.*

1. ВСТУП

У сучасних системах виявлення та попередження вторгнень як правило використовують методи, які зорієнтовані на два напрямки, а саме: перший напрямок спрямований на виявлення аномалій у системі, а інший – на пошук зловживань [1]. У переважній більшості систем попередження та виявлення вторгнень використовують поєднання різних рішень на базі синтезу відповідних методів. Це зумовлено тим, що два зазначені напрямки мають як переваги, так і недоліки.

Методи, які використовують для виявлення аномалій, ідентифікують процес, що викликав підозрілі відхилення чи зміни в роботі системи. Реалізація цієї ідеї дозволяє виявляти дії зловмисника, що має авторизовані права доступу в системі.

У цьому контексті існують дві групи методів, а саме: методи з контрольованим навчанням та з неконтрольованим навчанням. Характерною ознакою методів контрольованого навчання є те, що вказані методи використовують фіксований набір параметрів оцінки й апріорні відомості про значення параметрів оцінки, а також фіксований час навчання.

Що стосується неконтрольованого навчання, то в цьому випадку всі параметри оцінки можуть змінюватися із часом, крім того, сам процес навчання відбувається неперервно.

Методи, які належать до іншого напрямку, а саме виявлення зловживань, використовують механізми пошуку певних послідовностей подій, що визначаються як етапи реалізації вторгнень. І в цьому випадку застосовують контрольоване навчання.

Методи, які реалізовані в системах виявлення та попередження вторгнень, засновані на загальних уявленнях теорії розпізнавання образів. У цьому випадку для виявлення аномалій формується образ нормального функціонування системи, який базується на експертних оцінках. Указаний образ є певною сукупністю значень параметрів оцінки. І якщо відбувається зміна цього образу, то це трактується як аномальний стан системи.

Коли аномалії виявлені і проведена оцінка, то визначається природа цих змін, а саме: чи це просто допустиме відхилення, чи це результат вторгнення. Зазначені вище функції виконують системи виявлення та попередження вторгнень.

2. СТАН ПРОБЛЕМИ

Якщо атаку на інформаційну систему реалізує зловмисник високої кваліфікації, то це буде як правило багатокроковий процес. Тому одним із найпростіших способів злому системи або виведення її з дієздатного стану є використання сформованих модулів, які реалізують усі етапи атаки. Такі модулі мають назву "експлойти" і їх можна легко завантажити через інтернет.

Як відомо, системи виявлення та попередження вторгнень (Intrusion Detection System – IDS) мають два типи – це системи виявлення зловживань (Misuse Detection Systems – MDS) та системи виявлення аномалій (Anomaly Detection Systems – ADS).

Щодо систем MDS, то їхня робота ґрунтується на формуванні шаблонів атак. Рівень абстракції цих шаблонів атак може бути достатньо простим, якщо оперують інформацією про певні значення заголовків мережного пакета або послідовності певних команд у файлі аудиту, або достатньо складним. Якщо враховувати траєкторії системи у просторі станів під час проходження певних небезпечних станів, то в цьому разі система захисту може мати досить високу ефективність в тому випадку, коли буде відома схема атак. Але якщо вказана схема не буде відома, або атаки будуть мати непередбачувані відхилення від цієї схеми, тоді виникають проблеми. Тому звичайно в цьому випадку необхідно постійно актуалізувати базу даних кожної атаки та її можливих варіацій.

Можна зазначити, що в системах ADS певні дії, які є відмінними від поведінки в нормальному стані, ідентифікуються як аномальні. І це дає можливість реєструвати невідомі атаки в атакованій системі.

Системи ADS перед початком використання мають накопичити необхідну інформацію і скласти певну концепцію нормальної активності системи, чи окремих користувачів, або процесів. Ця концепція стає еталоном для оцінювання наступних дій і даних. У цьому випадку має бути визначена оптимальна сукупність факторів для спостереження. З одного боку їхня кількість не повинна знизити загальну продуктивність системи, а з іншого – для побудови профілю нормальної поведінки треба мати вичерпні характеристики цієї сукупності факторів.

Звичайно системи ADS не застраховані від помилок, які є двох видів:

а) користувач помилково приймається за зловмисника, або нормальна поведінка сприймається як зловмисні дії (англ. false positives);

б) за нормальну активність приймаються зловмисні дії чи спроба зловмисного проникнення в систему (англ. false negatives).

Друга помилка є небезпечніша за першу, і тому необхідно визначати умови, за яких ситуація може сприйматися як аномальна [2, 17].

Більшість спроб побудови ADS є концептуальними моделями, що перевіряють можливість застосування математичної моделі. А от реальних продуктів реалізації IDS мало і зазвичай це MDS.

З літературних джерел можна визначити типи методів виявлення аномалій, а саме:

а) частотні,

б) нейромережні,

в) на базі скінченних автоматів,

г) на базі зберігання прикладів поведінки,

д) спеціальні.

Отже як основне завдання можна визначити пошук найоптимальніших методів побудови ADS.

3. ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Формування образу нормального функціонування на базі сукупності певних параметрів для систем IDS характерно для методів виявлення аномалій, які саме і спрямовані на запобігання невідомим атакам і вторгненням.

Існує декілька способів формування образу нормального функціонування, а саме:

- для кожного параметра оцінки акумулюють характерну статистичну інформацію;
- нейронні мережі навчаються значенням параметрів оцінки;
- застосовують подієве подання.

У цьому випадку, як видно з переліку, у процесі виявлення сукупність параметрів відіграє ключову роль. Отже, головним завданням у цьому є визначення оптимальної множини, а також формування загального показника аномальності.

Для системи, яка підлягає захисту, у задачі вибору оптимальної сукупності ознак можна використати евристичний вибір сукупності параметрів вимірювань системи. Застосовуючи цей метод, можна досягти достатньо ефективного і точного розпізнавання вторгнень. Але треба брати до уваги той факт, що складові підмножини залежать від типів виявлених атак, тому для всього різновиду атак певний набір параметрів не підходить.

Кожна система має свій унікальний комплекс апаратно-програмних засобів і тому існує вірогідність, що IDS пропускає специфічні для даної системи вторгнення, які застосовують ідентичний набір параметрів.

Отже, визначати необхідні параметри оцінки доцільно у процесі роботи. Звичайно існують труднощі за динамічного формування параметрів оцінки. Ці труднощі пов'язані з тим, що області пошуку по експоненті залежать від потужності початкового набору параметрів.

Візьмемо певний початковий список з N параметрів, які є актуальними при передбаченні вторгнень. З урахуванням цього кількість підмножин даного списку буде становити 2^N. Ми бачимо, що в цьому випадку не є можливим для знаходження оптимальної множини використовувати алгоритми перебору. Тому одним із рішень може бути використання генетичних алгоритмів [3].

Треба зазначити, що оцінка аномальності має визначатися з розрахунку множини її параметрів. Для формування цієї загальної оцінки можливо використовувати метод, який базується на статистиці Баєса, або метод, заснований на використанні коваріантних матриць.

Використовуючи методи статистики Баєса зазначаємо, що A_1 ... A_n – це n вимірів. Ці виміри використовують для визначення в будь-який момент часу факту вторгнення. Оцінку різних аспектів системи, таких як кількість порушень пам'яті чи подій вводу-виводу, позначимо A_i.

Позначимо, що A_i може мати значення 1 – аномальне вимірювання, 0 – неаномальне вимірювання. У цьому випадку I беремо як гіпотезу того, що в системі є процес вторгнення.

Показники достовірності й чутливості кожного виміру визначають таким чином:

$$P(A_i = 1 \mid I) \text{ и } P(A_i = 1 \mid \neg I). \quad (1)$$

Далі за теоремою Баєса ймовірність обчислюється як

$$P(I \mid A_1, A_2, \dots, A_n) = \\ = P(A_1, A_2, \dots, A_n \mid I) \frac{P(I)}{P(A_1, A_2, \dots, A_n)}. \quad (2)$$

Для будь-якої комбінації множини вимірів треба обчислити умовну ймовірність для подій I.

Припускаємо, що кожне з вимірювань A_i залежить тільки від I і також умовно від інших вимірів не залежить, а саме A_j, де $i \neq j$.

Враховуючи зазначене вище, напишемо такі співвідношення:

$$P(A_1, A_2, \dots, A_n \mid I) = \prod_{i=1}^{n} P(A_i \mid I) \quad (3)$$

і

$$P(A_1, A_2, \dots, A_n \mid -I) = \prod_{i=1}^{n} P(A_i \mid \neg I), \quad (4)$$

тому

$$\frac{P(A_1, A_2, \dots, A_k \mid I)}{P(A_1, A_2, \dots, A_k \mid I)} = \frac{P(I) \prod_{i=1}^{n} P(A_i \mid I)}{P(I) \prod_{i=1}^{n} P(A_i \mid I)}. \quad (5)$$

Для визначення ймовірностей вторгнень використовують значення вимірювань аномалій, а також значення ймовірності появи кожного з вимірів аномальності, що були зафіксовані раніше, та ймовірність вторгнення.

Треба зазначити, що для більш реалістичної оцінки P ($I|A_1 \dots A_n$) треба врахувати вплив певних вимірювань A_i один на одного.

Ще один із методів, який допоможе враховувати зв'язки між вимірами, є коваріантні матриці. У цьому випадку, якщо виміри A_1 ... A_n являють собою вектор A, то

$$A^T C^{-1} A. \quad (6)$$

У цій формулі C є коваріантною матрицею, яка представляє залежність між кожною парою вимірів аномалій.

Далі розглянемо так звані мережі довіри чи мережі Баєса. Зазначимо, що вказані мережі – це графові моделі ймовірнісних і причинно-наслідкових зв'язків між змінними в статистичному інформаційному моделюванні. У цьому

випадку має місце поєднання емпіричних частот появи різних значень змінних, суб'єктивних оцінок "очікувань" і теоретичних уявлень про математичні ймовірності інших наслідків з апріорної інформації [4].

У цьому разі накопичені в певній спеціальній структурі вимірювання значень параметрів оцінки формують образ нормальної поведінки системи. Саме ця структура і називається профайлом. До структури профайла є ряд вимог. До головних можна віднести вимогу мінімального кінцевого розміру та вимогу до операції оновлення, яка повинна виконуватися як можна швидше.

Зазвичай застосовують статистичні методи оцінювання у разі виявлення можливих аномалій із використанням профайла. У цьому випадку в процесі виявлення відбувається порівняння поточних значень вимірювань профайла із збереженими значеннями. Таким чином визначається показник аномальності при вимірюванні.

Слід зазначити, що загальний показник аномальності в деякому простому випадку може обчислюватися з використанням загальної функції, враховуючи значення показника аномалії в кожному з вимірювань профайла. Як приклад можемо використати M_1, M_2 ... M_n, – вимірювання профайла, а S_1, S_2 .... S_n відповідно – значення аномалії кожного з вимірювань. І треба врахувати те, що чим більше число S_i, тим більше аномалій в i-му показнику.

Отже в цьому випадку об'єднувальна функція може бути вагою сум їхніх квадратів:

$$a_1 s_1^2 + a_2 s_2^2 + \ldots + a_n s_n^2 > 0, \qquad (7)$$

де a_i показує відносну вагу метрики M_i.

А якщо припустити, що параметри M_1, M_2 ... M_n, залежать один від одного, то в цьому випадку для їхнього об'єднання може знадобитися складніша функція.

Основна перевага такого підходу ґрунтується на застосуванні відомих статистичних методів.

Ще один спосіб формування образу нормальної поведінки – це використання нейронних мереж для навчання значенням параметрів оцінки.

Що стосується навчання нейронної мережі, то в цьому випадку застосовують послідовність команд, і будь-яка із цих команд може бути на більш абстрактному рівні, ніж використовувані параметри оцінки.

Нейронною мережею обробляють вхідні дані, які складаються з поточних команд і минулих W команд, які ще мають назву розміру вікна. Мережа являтиме собою образ нормальної поведінки, тільки після того, як дана нейронна мережа буде навчена множиною послідовних команд системи або хоча б однієї з її підсистем.

Фактично виявляється відмінність у поведінці об'єкта і передбачається визначення показника неправильно передбачених команд. І саме це є процесом виявлення аномалій.

На рисунку стрілки на рівні рецептора показують вхідні дані останніх W команд, які виконані користувачем.

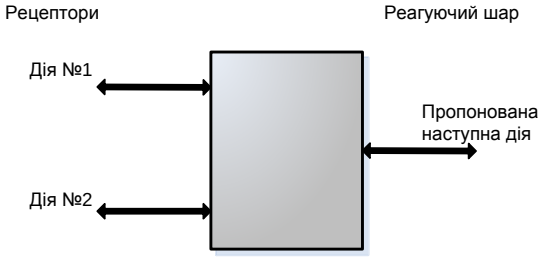

Рисунок. Концептуальна схема нейроних мереж IDS

У цьому випадку кілька значень або рівнів задає вхідний параметр. У свою чергу кожен із цих рівнів чи значень унікально визначає команду. А вихідний реагуючий багаторівневий шар передбачає наступну можливу команду користувача [5].

Щодо переваг указаного методу, то слід заначити, що нейронні мережі достатньо легко справляються з викривленими даними і крім того, враховують зв’язки між різними вимірюваннями, що впливають на результат оцінювання, причому роблять це автоматично. Підкреслимо, що успіх цього підходу не залежить від природи вихідних даних.

Звичайно, крім переваг метод має і недоліки, а саме: величезне значення має величина розміру вікна IDS та визначення топології мережі і ваги вузлів, що реалізуються після великої кількості спроб і помилок.

Далі розглянемо генерацію патернів. У цьому випадку представлення образу базується на певному припущенні про те, що можна пов’язати з поточним станом системи поточні параметри оцінювання. З урахуванням цього припущення функціонування можна подати у вигляді послідовності подій і станів.

У роботі [6] запропоновано певні тимчасові правила, які характеризують сукупності значень патерну (параметрів оцінювання) нормальної роботи. Крім того, ці правила можуть динамічно змінюватися на кращі правила у процесі навчання і їхнє формування відбувається індуктивно. Що стосується кращих правил, або так званих "хороших правил", то тут можна розуміти такі правила, які мають більшу ймовірність їхньої появи і крім того мають великий рівень унікальності для системи захисту.

Із сказаного вище можемо для прикладу записати таке правило:

$$E_1 \geq E_2 \geq E_3 \Rightarrow (E_4 = 95\%, E_5 = 5\%), \quad (8)$$

де $E_1 \ldots E_5$ – подія з безпеки.

З урахуванням зазначеного твердження доходимо висновку, що встановилася певна залежність для послідовності патернів, а саме: якщо маємо E_1, а далі E_2 та E_3, то після цього вірогідність прояву E_4 відповідно має 95 % , а E_5 усього 5 %.

Указані правила під час спостереження роботи користувача створюються індуктивно.

Якщо маємо таку ситуацію, що спостережувана послідовність подій відповідає лівій частині правила, виведеного раніше, а події, які відбулися в системі після цього, значно відрізняються від тих, які мали настати за правилом, то в такому випадку аномалія реєструється.

Отже стосовно переваг цього методу, можна зазначити, що він може ефективно визначати вторгнення з урахуванням залежності між подіями та їхньою послідовністю. Крім того, ураховуючи, що правила у вказаному методі містять у собі семантику процесів, то він має кращу чутливість до виявлення порушень. Також цей метод має кращу обробку користувачів, які мають чітку послідовність патернів, хоча можуть містити великі коливання поведінки. І безумовно перевагою такого методу є те, що він акцентує увагу не на всю підозрілу сесію, а на певні важливі події.

Треба звичайно зазначити і недолік указаного підходу, який пов’язаний із тим, що певні невпізнані патерни поведінки можуть бути не прийняті за аномальні тому, що вони не мають відповідності жодному з правил.

Звичайно використання методів виявлення аномалій не дає абсолютної гарантії з виявлення всіх вторгнень, тому системи IDS використовують окрім технології виявлення аномалій і технологію розпізнавання зловживань. У цій технології процес виявлення вторгнень базується на прогнозі з визначення можливих атак, і далі відбувається спостереження за їхньою появою [1, 13].

Під час застосування технології розпізнавання зловживань на відміну від технології виявлення аномалій образ є необхідним для подання несанкціонованих дій зловмисника і він не буде моделлю нормальної поведінки системи. Отже такий образ має назву сигнатура вторгнень. І ця сигнатура формується на значеннях параметрів оцінювання, а саме на основі тих же вхідних даних, що і в разі виявлення аномалій.

Слід зазначити, що ці сигнатури вторгнень визначають умови та спорідненість між подіями, які можуть призвести до певних зловживань. Крім того, дані сигнатури є корисними у виявленні спроб вчинення незаконних дій. Важливий аспект полягає в тому, що за наявності часточкового збігу сигнатур можна ідентифікувати спробу вторгнення.

Отже, для визначення можливих зловживань необхідно розрахувати умовну ймовірність. Позначимо так: *P (Вторгнення | Патерн подій).*

У цьому випадку використовуємо формулу Баєса для визначення ймовірності того, що якась множина подій є діями зловмисника:

$$P(I \mid A_1, A_2, \ldots, A_n) = \\ = P(A_1, A_2, \ldots, A_n \mid I) \frac{P(I)}{P(A_1, A_2, \ldots, A_n)}, \quad (9)$$

де I – вторгнення, а $A_1 \ldots A_n$ – послідовність подій.

Саме сукупність параметрів системи і є певною подією.

Для розв'язання задач із виявлення вторгнень також застосовують продукційні системи, перевагою яких є можливість поділу причин і рішень виниклих проблем.

Ця система, використовуючи правила if (якщо), причина then (то), рішення кодує інформацію про вторгнення. А саме у частині (if) правила кодують умови (причини), необхідні для атаки, і коли всі умови виконано, то виконується дія (рішення), задана у правій частині [7, 12].

Що стосується проблем, які можуть виникати під час використання певних додатків, які ґрунтуються на вказаному методі, то слід зазначити їхню недостатню ефективність у роботі з великими обсягами даних і складність у врахуванні залежної природи даних параметрів оцінки. Крім того, є проблеми з тим, що відсутня вбудована або природна обробка порядку послідовностей в аналізованих даних. Також прийнятність вбудованої експертизи залежить від того, чи певні модельовані навички адміністратора безпеки не є суперечливими.

Слід також зазначити, що під час використання продукційних систем об'єднання різних вимірів вторгнень і створення пов'язаної картини вторгнення призводить до того, що деякі причини стають невизначеними. Але все-таки за допомогою наявних даних можна встановити символічний прояв вторгнення. Хоч у вказаних системах виявляються лише відомі вразливості.

Ще один метод, а саме метод аналізу станів, був описаний у публікації [8] і його реалізація наведена в публікації [9]. У цьому випадку сигнатура вторгнень представляється послідовністю переходів між станами системи. А також патерни атаки пов’язані з певним станом системи і звичайно пов’язані із цим станом певною логічною

функцією. Можна вважати, що система вже перебуває в певному стані, якщо функція виконується. Необхідними подіями для наступних переходів є певні стани, які з'єднані з поточним лініями і при цьому певні типи подій, які можуть відбутися, є вбудованими в модель і як правило відповідають за принципом один до одного значенням параметрів оцінки.

Але слід зазначити, що певні патерни атак тільки задають послідовність подій і тому складніші способи визначення подій не можливі. Отже в цьому випадку використовується проста вбудована логічна функція.

Ще одна технологія, яка використовується для виявлення вторгнень – технологія спостереження за натисканням клавіш. У цій технології відбувається моніторинг натискань на клавіатурі певним користувачем для того, щоб ідентифікувати атаки. Отже в цьому випадку послідовність таких натискань користувачем є патерном атаки.

Проте на жаль під час використання такого підходу є проблема з надійністю механізму перехоплення роботи з клавіатурою, особливо коли відсутня підтримка операційної системи. Крім того, може бути велика кількість варіантів представлення ідентичних атак.

Ще одним слабким місцем цієї технології є те, що різного роду псевдоніми команд без використання семантичного аналізатора натискань просто зруйнують дану технологію. Причому досить складно буде виявити автоматизовані атаки, які є результатом виконання програм зловмисника [10, 14].

Ще одну групу методів для виявлення вторгнень, які застосовуються в IDS-системах, засновано на моделюванні поведінки зловмисника. У цьому випадку для виявлення зловживань можна використовувати метод об'єднання моделі зловживання з очевидними причинами, який використовує базу даних певних сценаріїв атак із послідовністю поведінок, що характерні для атаки.

Звичайно існує можливість, що кожна з підмножин у сценарії атак може бути присутня в системі. Результатом пошуку певної інформації в записах аудиту про наявність цих сценаріїв атак є певна кількість фактів, яка або підтверджує, або спростовує гіпотези.

Процес, в якому виконується перевірка, має назву антисепатор, і вказаний процес формує певну множину поведінок, базуючись на активній моделі, яка функціонує в поточний момент часу. Ця наступна можлива множина поведінок має бути перевірена у записах аудиту і тільки після цього буде передана планувальнику. Саме планувальник має визначити, яким чином має відобразитись у записах аудиту ця передбачена множина поведінок і сформувати певний системний вираз, який залежить від аудиту. Дані вирази повинні мати достатньо високу ймовірність того, що вони з’явилися б у записах аудиту, і крім того, такі структури, мають давати можливість легкого їх знаходження.

Отже, якщо у деяких сценаріїв підстави підозр збільшуються, а в інших сценаріїв зменшуються, то в цьому випадку йде мінімізація списку моделей активностей. Крім того, у такому списку може відбуватися оновлення ймовірностей появи сценаріїв атак за рахунок убудованого в систему обчислення причин [11, 16].

Що стосується переваг цього методу, то варто зазначити, що для одного запису аудиту є можливість мінімізувати кількість обробок, тобто більш явні події спочатку спостерігаються пасивно, а далі відбувається їхнє уточнення у разі підозри на загрозу. Також важливим моментом є те, що присутня незалежність у поданні даних аудиту в певній формі, і ця можливість забезпечується планувальником.

Відносно недоліків указаного методу, звичайно необхідно розробнику формувати точні кількісні характеристики для різних частин графічного представлення моделі, і це є суттєве додаткове навантаження. Зауважимо, що безумовно цей підхід тільки доповнює підсистему виявлення аномалій, а не змінює її. Крім того, не існує програмного прототипу, який би демонстрував ефективність цього підходу.

4. ВИСНОВКИ

Сучасні системи виявлення та запобігання вторгнень мають дві групи недоліків, а саме: недоліки, які пов’язані зі структурою систем, і недоліки, які пов’язані реалізованим методом виявлення вторгнень.

Що стосується недоліків, які пов’язані зі структурою системи виявлення вторгнень та запобігання їм, то можна зазначити деякі з них:

- загальна методологія побудови відсутня [26];
- прив’язка до конкретного обладнання систем IDS;
- складність установки IDS;
- складність оновлення IDS новими технологіями виявлення;
- виявлення методами системи зрозумілих атак може призводити до ряду незадовільних наслідків;
- оцінювання продуктивності в реальних умовах для IDS є складною задачею.

Також можна зазначити недоліки методів виявлення, які є в системах виявлення вторгнень та запобігання їм:

- наявність пропусків атак і помилкових спрацьовувань;
- складності в ідентифікації атакуючого та цілей атаки;
- складність виявлення вторгнень у реальному часі;
- складності у виявленні нових атак;
- низький рівень виявлення вторгнень на початкових етапах;
- відсутність критеріїв ефективності результатів роботи;
- відсутність можливості виявляти вже відомі атаки з модифікованими або новими стратегіями;
- складність в автоматичному виявленні координованих складних атак;
- перевантаження системи.

Отже можна дійти висновку, що для вдосконалення систем IDS необхідно акцентувати увагу на напрямках, які пов’язані з використанням методів теорії аналізу та синтезу інформаційних систем та апарату теорії розпізнавання образів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] J. Allen, A. Christie, W. Fithen, J. McHuge, J. Pickel, E. Stoner, "State of Practice of intrusion detection technologies", Technical Report CMU/SEI-99-TR-028. Carnegie Mellon Software Engineering Institute, 2000.

[2] Amrit Pal Singh, Manik Deep Singh, "Analysis of Host-Based and Network-Based Intrusion Detection System", India: Computer Network and Information Security, Vol. 8. pp.41–47, 2014.

[3] R. Heady, G. Luger, A. Maccabe, M. Servilla, "The Architecture of a Network Level Intrusion Detection System", Technical report, Department of computer since, University of New Mexico, August 1990.

[4] B. Balajinath, S. Raghavan "Intrusion detection through learning behavior model", Computer Communications, vol. 24, no. 12, pp. 1202–1212, 2001.

[5] H. Debar, M. Becker, D. Siboni. "A neural network component for intrusion detection systems", In proceeding of the 1992 IEEE Computer Society Symposium on Research in Security and Privacy, pp. 240–250, Oakland, CA, USA, May 1992.

[6] K. Cheng. "An Inductive engine for the Acquisition of temporal knowledge", Ph. D. Thesis, Department of computer science, university of Illinois at Urbana-Champain 1988.

[7] P. Porras, P. Neumann, "EMERLAND: Event Monitoring Enabling Response to Anomalous Live Disturbance", Proceeding of the IEEE Symposium on Research in Security and Privacy, Oakland, CA, May 1997.

[8] K. Ilgun, R. Kemmerer, P. Porras, "State Transition Analysis: A Rule-Based Intrusion Detection System", IEEE Trans. Software Eng. vol. 21, no. 3, Mar. 1995.

[9] K. Ilgun, "USTAT: A Real-time Intrusion Detection System for UNIX", Proceeding of the IEEE Symposium on Research in Security and Privacy.

[10] T. Heberlein, G Dias, K. Levitt, B. Mukherjee, J. Wood. "A network security monitor", In Proceeding of the 1990 IEEE Symposium on Research in Security and Privacy, pp. 296–304.

[11] T. Garvey, T. Lunt, "Model-based Intrusion Detection", Proceeding of the 14 th Nation computer security conference, Baltimore, MD, October 1991.

[12] S. Toliupa, I. Parkhomenko "The development of a process planning model of rational modular composition of the information protection systems" 2016 3rd International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S and T 2016 – Proceedings, 2017, pp. 159–162, 7905367

[13] Z. Bankovic, D. Stepanovich, S. Bojanic, O. Nieto-Taladris, "Improving network security using genetic algorithm approach", Computers and Electrical Engineering, vol. 33, no. 5-6, pp. 438–451, 2007.

[14] S. Toliupa, M. Brailovskyi, and I. Parkhomenko, "Building intrusion detection systems based on the basis of methods of intellectual analysis of data", IAPGOS, vol. 8, no. 4, pp. 28-31, Dec. 2018.

[15] Z. Bankovic "Improving network security using genetic algorithm approach", Computers and Electrical Engineering, vol. 33, no. 5-6., pp. 438–451, 2007.

[16] J. Anderson, "Computer Security Threat Monitoring and Surveillance", Developer Works, IBM, 19 Mart 2013

[17] A. Tajbakhsh, M. Rahmati, A. Mirzaei, "Intrusion detection using fuzzy association rules", Applied Soft Computing, vol. 9, no. 2, pp.462–469, 2009.

Стаття надійшла до редколегії 15.05.2021

Intrusion detection methods in modern IDS systems

Currently, the problem of protection of information and communication systems and resources of cyberspace is acute. The rapid development of the information sphere also leads to the modernization and complexity of methods of attacking cyberspace objects. The statistics of successful attacks on computer systems of various organizations, including government agencies, are growing every year. From this we can conclude that even the most reliable protection systems do not give a 100% guarantee of protection. One of the possible reasons for this state of affairs may be the use of standard security mechanisms and methods by most security systems. Such mechanisms include access delimitation based on the rights of the access subject, encryption and identification and authentication. Traditional methods cannot protect against their own users who have criminal intent. In addition, this approach does not solve the problem of clear division of existing system entities for authorized use of globalized resources, the ability to select passwords using specialized software, and the problem of limiting access to information system resources, which can result in reduced performance and complexity passing transactions between components of this system. Thus, there is a need to use mechanisms that would not reject the advantages of traditional ones, but also complement them. Namely, that these mechanisms detect attempts at unauthorized, unauthorized access, provide information about these attempts, and also be able to respond. One of the key factors in the use of such protection systems is their ability to prevent attacks by attackers who have been authenticated and authorized in accordance with all procedures and access rules and have obtained the necessary rights to certain actions. Of course, it is impossible to predict a complete set of event scenarios in a system with an authorized user who has malicious intent, but it is necessary to make a detailed description of possible "malicious" scenarios, or go back and describe the so-called "normal" scenarios. The description of normal scenarios will make it possible to detect dangerous activity, because this activity will deviate from the so-called "normal" scenario of behavior in the system, even by an authorized user. Thus, exploring the possibility of using mechanisms that are aimed at detecting anomalies in the system, or to search for abuses can help implement effective solutions for intrusion detection and prevention systems.

Keywords: *startup, cyberspace, cybersecurity projects, information technology, risks, IT products, fuzzy sets.*

Наталія Лукова-Чуйко,
доктор технічних наук, професор, завідувач кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка.

Natalia Lukova-Chuiko,
Doctor of Technical Sciences, Professor, Head of the Department of Cybersecurity and Information Protection of the Kyiv National Taras Shevchenko University.

Сергій Толюпа,
доктор технічних наук, професор кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка.

Serhii Toliupa,
Doctor of Technical Sciences, Professor of the Department of Cybersecurity and Information Protection, Taras Shevchenko National University of Kyiv.

Іван Пархоменко,
кандидат технічних наук, доцент кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка.

Ivan Parkhomenko,
Candidate of Technical Sciences, Associate Professor of the Department of Cybersecurity and Information Protection, Taras Shevchenko National University of Kyiv.