5. Егоров Ф. И. Вычислительные модули для системы защиты информации / Егорова Ф. И., Орленко В. С., Хорошко В. А. // Зб. наук. праць ВІКНУ ім. Т. Шевченко, Вип. № 11, 2008. – с. 117–124.

Рецензент: Дудивекич В.Б.
Поступила 20.12.2011

УДК 681.14:004.681.3

Хорошко В.О., Чернишев О.М.
ДУІКТ

АЛГОРИТМ ВИЯВЛЕННЯ АТАК ДЛЯ ЗАСОБІВ МОНІТОРИНГУ ІНФОРМАЦІЇ

Вступ

Високий рівень інформації, що характеризує сучасне суспільство, обумовлює залежність його безпеки від захищенності інформаційних технологій які використовуються. Широке застосування систем обробки інформації (СОІ), дозволяє вірішувати задачі автоматизації процесів обробки постійно зростаючих об'ємів інформації, зробило ці процеси особливо вразливими по відношенню до атакуючих впливів, що породило нову проблему- інформаційну безпеку.

Досвід експлуатації СОІ показує, що проблема інформаційної безпеки ще повністю не вирішена, з огляду на те, що засоби і методи захисту не в змозі запобігти атакам, кількість яких постійно зростає. Необхідна розробка нових підходів до створення засобів захисту інформації, здатних забезпечити адекватну протидію загрозам і задовольнити постійно зростаючим вимогам до безпеки СОІ і мереж.

Одним з ключових механізмів захисту інформації в СОІ і мережах є засоби моніторингу безпеки, які реалізують нагляд, аналіз і прогнозування станів безпеки СОІ і мережі. Вони виконують попередній аналіз, оперативний контроль і реалізацію механізмів реакції на вторгнення в СОІ і мережі, що забезпечує виявлення атак і попереджуюче формування комплексу заходів по локалізації можливих несанкціонованих дій в системі.

Ефективність системи моніторингу безпеки СОІ (СМБ СОІ) багато в чому визначається коректністю реалізації. Одним з найважливіших її елементів є алгоритм оцінювання стану об'єкту, що контролюється, для формування реакції засобів моніторингу безпеки на потенційно небезпечні дії в системі [1,2].

Таким чином, всебічний аналіз сучасних СМБ потребує оцінки властивостей алгоритмів формування імовірності вторгнень в СОІ, що використовуються при реалізації засобів моніторингу безпеки [3].

В теперішній час існує декілька основних підходів до реалізації засобів моніторингу безпеки [4], які використовують: статистичний аналіз, експертні системи і штучні нейронні мережі.

В цілому, для всіх відомих підходів до побудови СМБ СОІ характерні наступні недоліки:

- Існуючі СМБ не здатні точно ідентифікувати зловмисника, визначити його кінцеву ціль і мотив вчинків. В загальному випадку вони лише блокують дії зловмисника, що в майбутньому може призвести до повторних атак [5].
- Алгоритми формування імовірності вторгнення в СМБ СОІ і мережі оперують скороченним вектором небезпечних дій, що сформовані лише на основі данних самої системи.

- При визначенні імовірності вторгнення зловмисників в СОІ або мережу не виконується автоматичне ранжування загроз їх дій шляхом аналізу потенційних збитків системи.

- Події, що пов'язані з безпекою СОІ, ініціатори яких не виявленні , в подальшому ігноруються [6].

Алгоритми формування ймовірностей вторгнення не передбачають прогнозування дій порушника, що дозволяє сформувати «хибні вразливості» для зловмисника.

Ціль роботи

Таким чином, розробка нових алгоритмів аналізу ймовірностей вторгнень в СМБ, що дозволяють усунути або суттєво знизити відмічені раніше недоліки, є актуальною і представляється ціллю роботи.

Основна частина

На основі аналізу існуючих підходіві і алгоритмів моніторингу безпеки пропонується новий алгоритм оцінки імовірності вторгнення в СОІ або мережу, в якому враховуються цілі зловмисників і виконується групування їх дій за певними ознаками.

В даному алгоритмі для формування імовірності в СОІ використовується розширений сеансовий вектор $X = \{x_1, x_2, \ldots, x_n\}$, що являє собою лічильник факторів різноманітних загроз безпеки x_i, що зафіксовані засобами збору інформації і перевірки стану СОІ чи мережі.

В існуючих підходах векторХ характеризується дублюванням факторів і, як наслідок, їх надмірністю, а також високою деталізацією параметрів загроз, які враховуються, що ускладнює подальшу його обробку. В запропонованому алгоритмі виконується групування факторів x_i окремих, в тому числі низькорівневих, дій зловмисника в більш високорівневі події порушення безпеки і формується вектор дій А (див. рис.1).

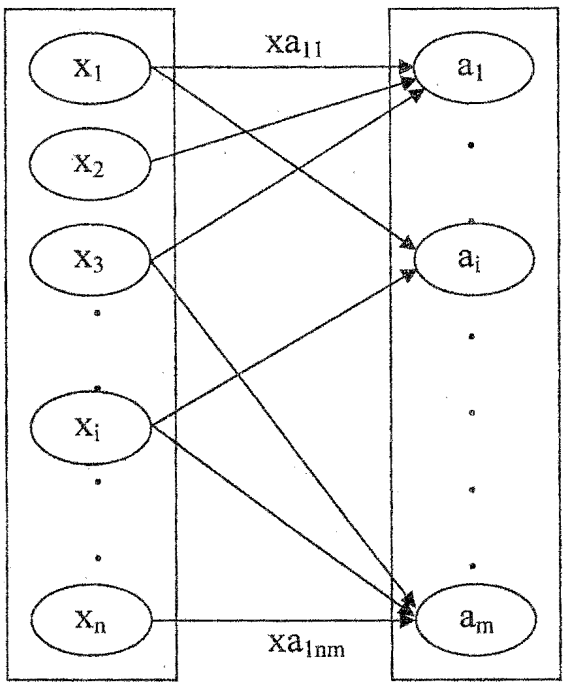

Рис.1. *Групування елементів вектору Х в вектор дій А*

Елементи вектору А розраховуються як

$$a_j = \sum_{i=1}^{n} x_i xa_{ij}, \qquad (1)$$

де xa_{ij} – елемент матриці перетворення

$$XA = \begin{bmatrix} xa_{11} & \cdots & xa_{1m} \\ \vdots & \cdots & \vdots \\ x_{ni} & \cdots & xa_{nm} \end{bmatrix}$$

при цьому xa_{ij} – коефіцієнт, відповідний вазі фактору x_i в кінцевій дії a_j суб'єкту.

В загальному вигляді вираз (1) можна записати у вигляді:

$$A=Fxa(X), \qquad (2)$$

де Fxa – функція перетворення вектору X в вектор A.

Формування вектору $A= \{a_1, a_2, ..., a_m\}$ у відповідності з (1) дозволяє мінімізувати об'єм інформації, що обробляється за рахунок групування факторів дій суб'єктів і при цьому більш коректно аналізувати її у порівнянні з використанням звичайного порогового вектору X.

Спочатку коефіцієнт xa_{ij} визначається на основі статистичних даних про дії суб'єктів в СОІ і експертних оцінок, потім він автоматично оновлюється за наступним принципом: коефіцієнт xa_{ij} того фактору x_i, який виявляє більший/менший вплив при здійсненні відповідної дії a_j, збільшується/зменшується на величину Δ_{ij} у відповідності до формули

$$xa_{ijнов} = xa_{ij} + \Delta_{ij}, \qquad (3)$$

$$\Delta_{ij} = \frac{x_{iнно} - x_i}{a_j}\delta, \qquad (4)$$

де Δ_{ij} – корекція ваги фактору x_i, у дії a_j; $xa_{ij\ нов.}$ – значення ваги фактору x_i у дії a_j після корекції; у дії $x_{i\ нов.}$ – нове значення фактору x_i; δ – коефіцієнт настройки факторів.

Крім того, запропонований алгоритм дозволяє модифікувати склад груп факторів $\{x\}$ для вектору A, але рішення про включення/виключення факторів приймає адміністратор.

Таким чином, параметри вторгнення зображуються у вигляді кортежу даних

$\{s_1, ..., s_n\}$, $\{t_1, ..., t_c\}$, $\{l_1, ..., l_d\}$, $\{m_1, ..., m_e\}$, $\{\gamma_1, ..., \gamma_f\}$,

де s_i – суб'єкт ініціатор події, t_i – час події, l_i – місце події, m_i – задіяні засоби, γ_i – ступінь успішності вторгнення (атаки).

Далі проводиться імплікація дій суб'єктів в їх цілі (рис. 2).

Дане перетворення дозволяє прогнозувати можливий наступний крок суб'єкту за рахунок встановлення кореляційної залежності між ціллю q_j і набором дій {a}, необхідних для її досягнення.

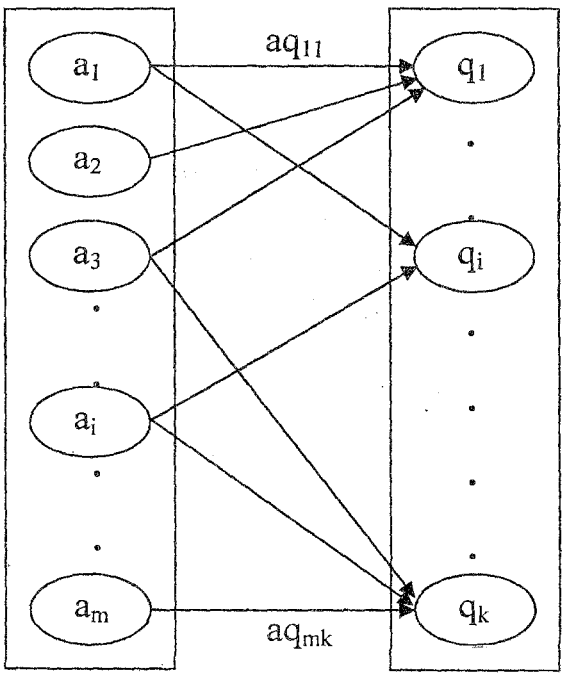

***Рис.2** Імплікація вектору А у вектор цілей Q*

Важливість виконання цього перетворення обумовлена тим, що набір формально не зв'язаних дій може переслідувати загальну ціль.

Елемент q_j вектору цілей Q розраховується як

$$q_j = \sum_{i=1}^{m} a_i aq_{ij}, \qquad (5)$$

де aq_{ij} – коефіцієнт, що показує всі дії a_i суб'єкту в досягненні цілі q_j. Даний коефіцієнт – це елемент вагової матриці AQ, яка формується на підставі експертних оцінок і статистичних даних про дії суб'єктів.

$$AQ = \begin{bmatrix} aq_{11} & \cdots & aq_{1k} \\ \vdots & \cdots & \vdots \\ aq_{m1} & \cdots & aq_{mk} \end{bmatrix}$$

Аналогічно оновленню коефіцієнтів xa_{ij} виконується автоматичне оновлення коефіцієнтів aq_{ij} на підставі статистики про дії суб'єктів в СОІ і мережах.

В загальному вигляді вираз (5) можна представити як

$$Q = Faq(A) \qquad (6)$$

де Faq – функція перетворення вектору А у вектор Q.

На наступному етапі на основі інформації про існуючі причинно-наслідкових зв'язки, що вказують на взаємозв'язок між вторгненням (атакою), диференційованими за часом, місцю, способу атаки і задіяним засобам, будується імовірнісний граф потенційних цілей зловмисника (рис. 3).

Даний граф описує послідовність потенційних цілей порушника для реалізації вторгнень (атак) [5]. Вершини графу q_i представляють собою цілі досягнення яких

дозволяє робити певний вплив на СОІ і мережі, а дуги ω_{ij} – імовірності, що показують ступінь можливості переходу від одної цілі до іншої.

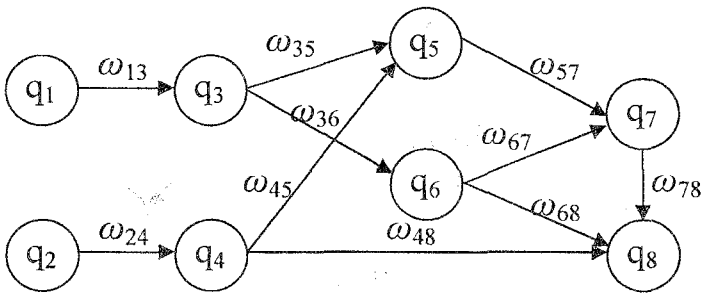

Рис. 3. *Імовірнісний граф потенційних цілей.*

Граф цілей дозволяє побудувати ланцюжок імовірних дій зловмисника, виходячи з його поточного положення у просторі цілей і поточної активності, а також спрогнозувати його наступні кроки і визначити потенційні і можливі кінцеві цілі і, відповідно, можливі дії.

Так, якщо відомі потенційні цілі зловмисника, то відповідні їм дії a_i можуть бути отримані із

$$A = F_{aq}^{-1}(Q), \tag{7}$$

а фактори x_i різних загроз безпеки, які при цьому необхідно контролювати, з

$$X = F_{xa}^{-1}(A), \tag{8}$$

де F_{aq}^{-1} і F_{xa}^{-1} - функції зворотного перетворення відносно функцій F_{aq} і F_{xa}, відповідно.

Отриманий прогноз поведінки зловмисника може бути використаний для емуляції уразливостей і системних відомостей (маскарад). Причому в залежності від характеру дій і цілей зловмисника можуть застосовуватися як приховані і дезінформація, так і повна підміна критичних даних.

Задача засобів захисту інформації складається в забезпеченні безпеки інформаційних ресурсів СОІ. Таким чином, необхідно встановити відповідність між цілями зловмисника і ресурсами, які будуть підвладні атакам при реакції цих цілей.

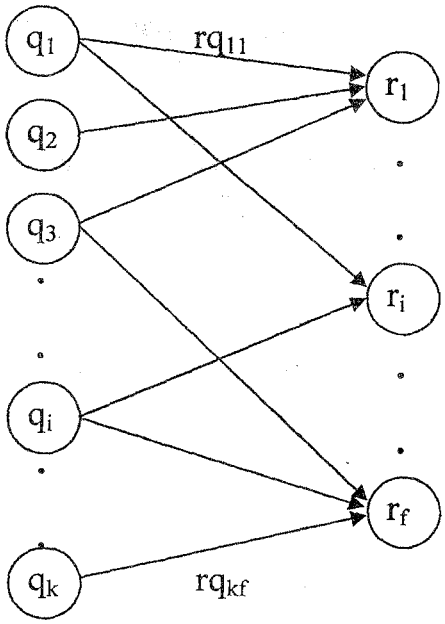

Рис. 4. *Відбиття набору цілей {q} на ресурси {r} COI.*

На рис.4 показано відбиття набору цілей *{q}* зловмисників на ті інформаційні ресурси *{r}* COI, які можуть бути підвладні атакам або впливам. Значення вектору конкретних інформаційних ресурсів

$$R_{1\times f} = Q_{1\times k} \times \left\| QR_{k\times f} \right\|, \qquad (9)$$

де $Q_{1\times k}$ – вектор цілей; $QR_{k\times f}$ – матриця перетворення, коефіцієнти qr_{ij} якої, відбивають вплив досягнутих зловмисником цілей q_i у впливі на інформаційний ресурс r_j COI.

На рис. 5 показано повний цикл перетворення дій зловмисника a_i за допомогою формування відповідних їм наборів цілей *{q}* в елементи вектору *{r}*, що відбивають ступінь загрози дій *{a}* суб'єктів для конкретних інформаційних ресурсів *{r}* COI.

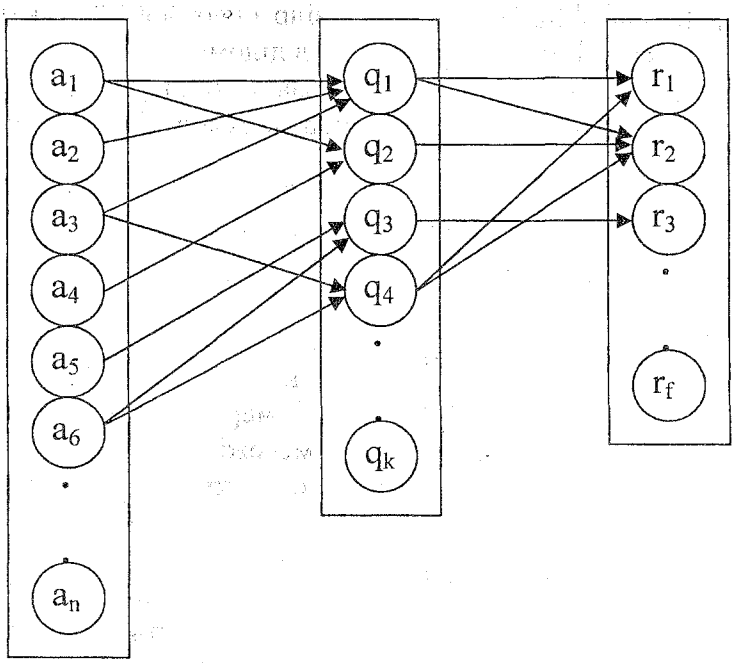

Рис. 5. *Залежність між діями порушника {a} і ресурсами {r} СОІ, що наражаються атакам*

Інформаційна цінність ресурсу r_1 визначається виразом [7]

$$r_1 = q_1 q r_{11} + q_4 q r_{41}, \qquad (10)$$

що еквівалентно

$$r_1 = (a_1 a q_{11} + a_2 a q_{21} + a_3 a q_{31}) q r_{11} + (a_3 a q_{34} + a_6 a q_{64}) q r_{41}. \qquad (11)$$

Інформаційна цінність r_i ресурсу прямо пропорційна імовірності вторгнення p_i зловмисника в СОІ.

Запропонований підхід дозволяє визначити потенційну цінність $r_{1\ нов}$, ресурсу r_i за допомогою імовірнісного графу цілей (див. рис. 3). Так, наприклад, якщо ціль q_4 ще не досягнута, то

$$r_{1нов} = r_1 + (q_2 + w_{24}) q r_{21}. \qquad (12)$$

Як видно із виразу (12), потенційна цінність даного ресурсу СОІ більше або дорівнює його поточній цінності.

Поточна інформаційна цінність ресурсу зменшується в тому випадку, якщо цілі і дії зловмисників не спрямовані на даний інформаційний ресурс.

Далі в запропонованому алгоритмі формується диференційна оцінка імовірності атаки p_i в СОІ і мережу, що враховує ранжування станів СОІ, яка визначається як імовірність впливу на ресурс r_i, з врахуванням коефіцієнту нормування κ_i

$$p_i = \kappa_i r_i \qquad (13)$$

Коефіцієнт нормування κ_i –параметр для приведення діапазону знань, отриманих при аналізі можливих впливів на інформаційний ресурс, до інтервалу [0…1]. Для

різноманітних ресурсів значення коефіцієнту κ_i відрізняються і залежать від їх цінності, критичності і важливості для роботи всієї системи в цілому.

На кінцевому етапі алгоритму збираються отримані по ряду сеансів роботи суб'єктів і визначається квота підозрілості дій зловмисників, а також формується ступінь загрози інформаційним ресурсам.

Запропонований алгоритм дозволяє ранжувати дії і цілі суб'єктів за ступенем їх загроз безпеці СОІ і мереж, що, в свою чергу, забезпечує диференційну оцінку імовірності атаки в залежності від цінності інформаційного ресурсу.

Висновки

Побудова якісних СМБ СОІ і мереж потребує використання ефективних алгоритмів для аналізу потенційних атак зловмисників в СОІ і мережах. Запропонований алгоритм формування імовірностей атак і вторгнень в СОІ і мережі забезпечує:

- підвищення захищеності користувацьких і системних даних за рахунок виконання прогнозування дій зловмисників і емуляції вразливостей і системних відомостей;
- гнучку реакцію СМБ на дії зловмисників;
- ранжування дій і цілей суб'єктів за ступенем їх загроз безпеці СОІ і мережам;
- зменшення об'єму системної інформації, яка аналізується, що дозволяє практично не знижувати продуктивність СОІ і пропускну здатність мереж.

Література

1. *Конеев И.Р. Информационная безопасность предприятия // Конеев И.Р., Беляев А.В. – СПб.: БВХ – Петербург, 2003ю – 752с.*
2. *Кузнецов О.О. Захист інформації в інформаційних системах // Кузнецов О.О., Євсеєв С.П., Король О.Г. – Харків: Вид. ХНЕУ, 2011.-512с.*
3. *Bace R. An Introduction to Intrusion Direction Assessment for System and Network // Security Management . – 2003, №7 – P 167-180.*
4. *Ленков С.В. Методы и средства защиты информации. В 2-х томах // Ленков С.В., Перегудов Д.А., Хорошко В.А. – Киев: Арий, 2008.*
5. *Кобозева А.А. Анализ информационной безопасности // Кобозева А.А., Хорошко В.А. – Киев: Изд. ГУИКТ, 2009.-251с.*
6. *Азаренко Ю.Ю. Мониторинг информации в компьютерных сетях // Азаренко Ю.Ю., Смычков Е.Е., Чернышев А.Н., Хорошко В.А. // Збірник наукових праць СНУЯЕтаП, №2(22), 2007.-с.187-197.*
7. *Азарова О.В. Оценка ценности и достоверности полученной информации // Азарова О.В., Дуршевич Я.В., Хорошко В.А. // Захист інформації, №3, 2005. - с. 73-78.*

Рецензент: Шокало В.М.
Надійшла 27.12.2011

УДК 004.056:621.396.67(045)

Ильницкий Л.Я., Пепа Ю.В., Осама Тураби
Национальный авиационный университет

ИСПОЛЬЗОВАНИЕ ПОЛЯРИЗАЦИИ ДЛЯ ПОВЫШЕНИЯ СКРЫТНОСТИ ПЕРЕДАЧИ ИНФОРМАЦИИ

Введение. Радиоконтроль за использованием радиочастот осуществляется с помощью сети фиксированных и мобильных станций. Последние представляют собой автомобили, оборудованные специальной измерительной аппаратурой и системой