DOI: https://doi.org/10.36910/6775-2524-0560-2023-53-18
УДК 004.023
Кардашук Володимир Сергійович[1], к.т.н., доцент
https://orcid.org/0000-0002-7440-6753
Бортник Катерина Яківна[2], к.т.н., доцент
https://orcid.org/0000-0001-5282-099X
Багнюк Наталія Володимирівна[2], к.т.н., доцент
https://orcid.org/0000-0002-7120-5455
[1] Східноукраїнський національний університет імені Володимира Даля, м. Сєвєродонецьк, Україна
[2] Луцький національний технічний університет, м. Луцьк, Україна

ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ У ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖАХ ТА ВІДБИТТЯ АТАК НА WEB-ДОДАТКИ

Кардашук В.С., Бортник К.Я., Багнюк Н.В. Проблеми захисту інформації у віртуальних приватних мережах та відбиття атак на Web-додатки.

У статті розглянуті сучасні проблеми захисту інформації у віртуальних приватних мережах, що використовують технологію VPN, стосовно масштабованості, гнучкості адміністрування, вимог до підключень та вартості. Для реалізації дослідження відбиття атака на WEB-додатки за допомогою евристичного методу проаналізована та досліджена нейронна мережа адаптивної-резонансної теорії. Запропонована модифікована структура, алгоритм навчання нейронної мережі та рішення щодо усунення недоліків її роботи. В результаті дослідження намічені подальші шляхи удосконалення алгоритму навчання нейронної мережі, що направлені на збільшення кількості відбиття атак на WEB-додатки

Ключові слова: приватна мережа, безпека програмного середовища, захист WEB-додатків, нейронна мережа, відбиття атак, алгоритм навчання**.**

Kardashuk V., Bortnyk K., Bahniuk N. Problems of protecting information in virtual private networks and defending attacks on Web-applications.

The article discusses the current problems of information protection in virtual private networks using VPN technology, in terms of scalability, flexibility of administration, connection requirements and cost. For the implementation of the study of the reflection of the attack on WEB-applications using the heuristic method, the neural network of the adaptive resonance theory was analyzed and researched. A modified structure, learning algorithm of the neural network and solutions to eliminate the shortcomings of its operation are proposed. As a result of the study, further ways of improving the learning algorithm of the neural network aimed at increasing the number of repelling attacks on WEB applications are planned.

Keywords: private network, security of the software environment, protection of WEB applications, neural network, reflection of attacks, learning algorithm.

Актуальність дослідження. Virtual Private Network (VPN) є розширенням приватної мережі, що здійснює свою роботу через мережу Internet. VPN дає користувачам можливість послати дані між двома комп'ютерами по загальнодоступній або відкритій мережі в такій спосіб, що імітує властивості каналів зв'язку типу P2P (Peer-toPeer) [1]. Це робить віддалений комп'ютер фактично частиною приватної мережі шляхом створення зашифрованого тунелю в загальнодоступній мережі. Технологія VPN розв'язує проблеми, що супроводжують тенденцію до збільшення обсягу дистанційної роботи й широкому поширенню глобальних операцій, де співробітники повинні мати можливість з'єднуватися із центральними ресурсами й взаємодіяти один з одним.

Постановка проблеми. Традиційні методи з'єднання віддалених офісів з корпоративною мережею полягали в тому, що підключення працювало по загальній мережі, що комутується, PSTN (public switched telephone network), або використати спеціалізовану орендовану WAN (wide area network,), використовуючи фрейм-ретранслятор або синхронну схему протоколу PPP (Point-to-Point Protocol) [2]. Ці методи вимагають значних витрат часу на адміністрування й доволі не дешеві в обслуговуванні. Типова синхронна схема, що управляє фреймом-ретранслятором PPP або декількома PSTN лініями, становить істотні регулярні витрати компанії. Жодне із цих рішень не дає необхідної масштабованості в термінах вартості, гнучкого адміністрування й вимог до підключень. Тому має сенс замінити модемні пули й інфраструктуру приватних мереж менш дорогим рішенням, заснованим на технології Internet, щоб бізнес міг зосередитися на областях його основної компетенції. За допомогою Internet-рішення всього кілька інтернет-підключень через служби інтернет-провайдерів (Internet Service Provider або ISP) і комп'ютери VPN-серверів можуть обслуговувати потреби віддаленої роботи в мережі клієнтів і філій.

Метою статті є дослідження та розроблення евристичної системи захисту WEB-додатків, що має істотні переваги порівняно з існуючими на сьогоднішній день методами детектування і відбиття атак.

Аналіз останніх досліджень і публікацій. Діяльність, пов'язана з конфігуруванням і створенням VPN, відома як робота у віртуальній приватній мережі. Щоб емулювати зв'язок P2P, дані інкапсулюються або включаються у пакет, при цьому заголовок містить інформацію про маршрутизацію, дозволяючи даним перетинати загальнодоступну або відкриту мережу транзитом для досягнення місця призначення. Для емуляції приватного зв'язку й підтримки конфіденційності посилають данні, що зашифровані. Пакети, перехоплені в загальнодоступній відкритій мережі, передаються у зашифрованому вигляді і без ключів кодування їх неможливо відтворити. VPN-підключення дозволяють користувачам, що працюють віддалено, з'єднуватися безпечним способом з віддаленим сервером організації, використовуючи інфраструктуру маршрутизації, що забезпечується мережею Internet.

З погляду користувача VPN-підключення є прямим підключенням між комп'ютером користувача й сервером організації. Природа проміжної мережі несуттєва для користувача, тому що йому здається, начебто дані послані по спеціалізованому приватному зв'язку.

VPN дозволяє корпорації з'єднуватися з філіями або з іншими компаніями по загальнодоступній мережі (типу Internet) при підтримці високої безпеки зв'язку. В обох випадках безпечне підключення по міжнародній мережі виглядає для користувача як приватний зв'язок, незважаючи на те що цей зв'язок проходить по суспільній міжнародній мережі.

Щоб дати користувачам можливість з'єднуватися з обчислювальними ресурсами організації незалежно від їхнього місця розташування, корпорація повинна розгорнути масштабоване рішення віддаленого доступу. Як правило, корпорації вибирають або таке рішення, у якому внутрішньому відділу інформаційних систем поручається закупівля, установка й підтримка модемних пулів організації й інфраструктури приватної мережі; або вибирають VAN (value-added network) рішення, у якому вони оплачують субдоговір з іншими компаніями на купівлю, установку й обслуговування модемних пулів і інфраструктури телекомунікацій [3].

Вирішення проблеми. З використанням зв'язку між клієнтами на сервер організації або на сервер посередника мережного доступу NAS (network access server) [4], користувач під'єднується до інтернет-провайдера. VPN-клієнт створює VPN-підключення між комп'ютером віддаленого доступу й VPN-сервером організації по Internet. Використання VPN-технології дозволяє компанії скоротити щомісячні регулярні витрати на швидкодіючі схеми. Використання зв'язку через місцевого інтернет-провайдера на офісних сайтах і єдиної швидкодіючої схеми в загальному офісі дозволяє компанії зробити кілька швидкодіючих підключень, керування оверлеєм фрейму-ретранслятора, обслуговування архітектури маршрутизації WAN і пов'язані з ними істотні регулярні фінансові й адміністративні витрати.

Існує два методи використання VPN-технології для підключення локальних мереж на віддалених сайтах. Перший метод - завжди включена VPN. Використання виділених ліній для підключення філій до локальної мережі організації (LAN). Замість того щоб використати дорогу спеціалізовану схему між філіями й корпоративним центром, маршрутизатори як філій, так і центра можуть використати місцеву спеціалізовану схему й місцевий інтернет-провайдер для підключення до Internet. Програмне забезпечення VPN використовує підключення до місцевого інтернет-провайдера й Internet для створення VPN між маршрутизатором філії й центральним маршрутизатором компанії.

Другий метод - включення VPN за вимогою. Замість того щоб мати у філії маршрутизатор, що дозволяє робити з'єднання до корпоративного або NAS-серверу, маршрутизатор філії може викликати місцевого інтернет-провайдера. Маршрутизатор філії використає підключення до місцевого інтернет-провайдера для створення VPN-підключення між маршрутизатором філії й центральним корпоративним маршрутизатором по Internet.

В обох випадках засоби, що відповідають за з'єднання філій і центрального офісу із Internet, є локальними. Будь-який із цих підходів дозволяє корпорації уникнути додаткових витрат на зв'язок між клієнтами, пов'язаних з використанням PSTN-ліній, або витрат на орендований канал, тому що обидві сторони роблять ближні підключення орендованого каналу до свого інтернет-провайдеру. Інтернет-провайдер має справи із проблемами проміжного мережного зв'язку, із проблемами

інтернет-маршрутизації й дозволом імен сайтів, тобто всі складності вилучені з роботи глобальної мережі шляхом використання VPN-підключення між сайтами.

При використанні конфігурації VPN-підключення центральний корпоративний маршрутизатор, що діє як VPN-сервер, повинен бути пов'язаний з місцевим інтернет-провайдером по виділеній лінії, що завжди включена й приймає запити на підключення цілодобово.

Є багато ситуацій, коли корпорація хоче мати підключення тільки при необхідності, так що підключення можуть бути сконфігуровані або як "завжди включені", або як "включені за вимогою", які активізуються тільки при необхідності. В об'єднаних мережах деяких організацій частина відомчих даних настільки секретна, що місцева мережа відділу фізично роз'єднана з іншою частиною об'єднаної мережі організації. Таким прикладом можуть бути дані відділу кадрів компанії, що блокуються від загального доступу, або політика Microsoft, що складається в блокуванні даних, що стосується розробки серверів, від персоналу, що не входить у коло розробників.

По суті, найкращий спосіб гарантії того, що дані не будуть скомпрометовані, полягає в тому, щоб взагалі заборонити зв'язок, реалізуючи "повітряний зазор" між захищеними ресурсами й загальним мережним доступом. Хоча цей метод захищає конфіденційну інформацію відділу, він створює проблеми доступу до інформації для користувачів, не зв'язаних фізично з окремими локальними мережами. Технологія VPN забезпечує рішення, що дозволяє локальній мережі відділу зв'язуватися з об'єднаною мережею організації, але при цьому залишатися технічно екранованої й захищеної за допомогою VPN-сервера.

У цій конфігурації мережа фізично підключає екрановану мережу відділу до іншої частини корпорації. Однак використовуючи VPN-сервер як шлюз до мережевих ресурсів екранованого відділу, мережений адміністратор може гарантувати, що тільки ті користувачі об'єднаної мережі організації, які мають відповідні повноваження (credentials) (засновані на політиці необхідного рівня поінформованості в межах компанії), можуть встановлювати VPN-підключення з VPN-сервером і одержувати доступ до захищених ресурсів відділу.

Крім того, весь зв'язок між віддаленою робочою станцією й VPN-сервером може бути зашифрований для збереження конфіденційності даних. Шляхом використання VPN-сервера як шлюза, користувачі, що не мають належних повноважень, не можуть переглядати локальну мережу відділу, а користувачі, що мають належний дозвіл на доступ, можуть переглядати локальну мережу відділу з дотриманням повної таємності й захистом по внутрішній мережі компанії.

Таким чином, VPN дозволяє вирішити цілу низьку проблем пов'язану з забезпеченням комп'ютерної безпеки на сучасному етапі розвитку глобальних мереж.

Щодо проблеми створення безпечного середовища для функціонування WEB-додатків, слід зазначити, що не дивлячись на те, що у сучасному світі інформаційних технологій існує багато розробок, які покликані створити безпечне інформаційне середовище, створити повністю безпечне середовище для конкретного додатка вони ще не здатні. На сьогоднішній день створені надійні системи шифрування, безпечні канали доступу, високоефективні брандмауери, але кінцева точка мережі, яка являє собою у більшості випадків WEB-додаток, є слабо захищеною або незахищеною зовсім.

Провівши детальний аналіз відомостей про методи здійснення атак на WEB-додатки, багато фахівців в області безпеки сходяться в думці, що можливо створити обмежену безліч відбитків (сигнатур) атак, які можуть бути використані для виявлення тієї чи іншої атаки з досить високою ймовірністю.

На сьогоднішній день найбільш успішним і популярним програмним брандмауером, що спеціалізується на захисті WEB-додатків, є проект ModSecurity [5]. Цей брандмауер являє собою модуль для широко розповсюдженого WEB-сервера Apache. Модуль являє собою фільтр який перевіряє POST, GET і COOKIE параметри, які передаються між користувачем і віддаленим сервером у мережі Internet.

Варто зазначити, що ModSecurity вимагає кропіткого й точного налаштування за участю фахівця з безпеки WEB-серверу. Налаштування модуля "за замовчанням" не можуть використовуватися для захисту критичних до проникнення WEB-додатків (наприклад електронних банків або електронних магазинів).

Спробою створити найбільш повну конфігурацію для ModSecurity з урахуванням більшості можливих варіацій атак можна вважати рекомендації, опубліковані в [6]. Це полегшило роботу з

настроювання модуля, однак послуги фахівця для адаптації загальних рекомендацій з настроювання під конкретні завдання усе ще потрібні.

ModSecurity має істотний недолік – відсутність регулярного оновлення баз сигнатур атак. До недоліків цього модуля варто також віднести те, що він оперує лише жорстко заданими правилами й не має евристичних алгоритмів для детектування варіацій відомих атак і попередження нових типів атак. Крім того дії ModSecurity не враховують індивідуальних особливостей всіх WEB-додатків, які можуть обслуговуватися одним WEB-сервером.

У зв'язку з описаними вище недоліками існуючих рішень по захисту WEB-додатків запропоновано систему побудови захисту WEB-додатку і WEB-серверу, що реалізує евристичні можливості за допомогою масиву нейронних мереж адаптивно-резонансної теорії, які оперують двійковими даними. Система працює на сьомому рівні моделі OSI і, завдяки своїм унікальним властивостям, дозволяє не тільки ефективно боротися з існуючими типами атак, але й попереджати проведення нових типів атак. Основною перевагою системи є те, що вона не потребує оновлення бази сигнатур, бо будується на евристичному алгоритмі.

За основу дослідження обрана модель нейронної мережі адаптивно-резонансної теорії (АРТ) [7]. Серед безлічі вже відомих моделей нейронних мереж ця мережа схожа по своїй роботі з процесом мислення людини. Вона має здатність приймати рішення щодо подібності інформації, яка надійшла, з інформацією, що вже зберігається у пам'яті. Мережа АРТ-1 здатна приймати рішення на основі раніше отриманого досвіду (даних).

Базова архітектура мереж АРТ (рис. 1) включає три групи нейронів: поле F1 вхідних обробних нейронів, що складає із двох шарів елементів, шар Y-нейронів розпізнавальних нейронів і керуючий нейрон R. Архітектура мережі АРТ-1 крім наявності базової групи нейронів має додаткові зв'язки й елементи G1 і G2 (рис. 2).

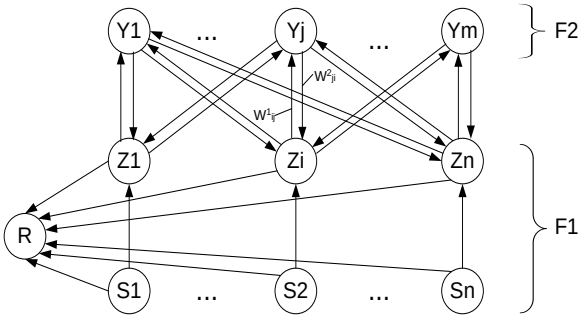

Рис. 1– Базова архітектура мережі АРТ

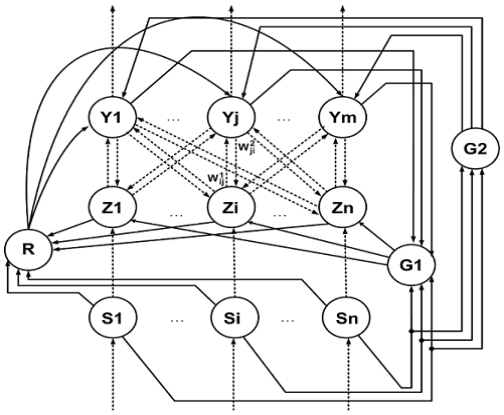

Рис. 2 – Архітектура нейронної мережі АРТ-1

Нейронна мережа адаптивної-резонансної теорії відносить вхідне зображення до одного зі сформованих класів у процесі навчання, якщо воно відповідає заданому критерію подібності й у достатньому ступені подібно із прототипом цього класу. Далі відбувається модифікація вхідного зображення для більшої відповідності із пропонованим зображенням – корегуються ваги зв'язків.

Поле F1 вхідних обробних нейронів складається із двох шарів – вхідного шару S-елементів і інтерфейсного шару Z-елементів. Вхідний шар сприймає пропоноване зображення й передає отриману інформацію нейронам інтерфейсного Z-шару й керуючому нейрону R.

Кожний елемент Zi (i = 1, ..., n) інтерфейсного шару пов'язаний з кожним елементом Yj (j = 1, …, m) шару, що розпізнає, з Y двома видами зв'язків. Сигнали з інтерфейсного шару до шару Y передаються зв'язками, що йдуть знизу нагору з вагою W1ij, а із розпізнавального шару до інтерфейсного – зв'язками ваги W2ji , (j = 1, …, m, i = 1, …, n).

Шар Y є шаром конкуруючих нейронів, що змагаються. У будь-який час кожний елемент Yj (j = 1, …, m) розпізнавального шару може перебувати в одному із трьох станів: 1 – активний, бере участь у змаганнях; 0 – неактивний, але нейрон може брати участь у змаганнях; –1 – загальмований, не бере участь у змаганнях при пред'явленні поточного зображення.

Після пред'явлення вхідного зображення активним залишається тільки один нейрон, що розпізнає (нейрон-переможець), всі інші Y-елементи мають нульові або негативні вихідні сигнали. Виділений нейрон, що розпізнає, допускається до навчання вхідним зображенням тільки в тому випадку, коли його ваговий вектор зв'язків із шару Y до шару Z подібний до вхідного вектору. Це рішення приймається за допомогою R-нейрона й параметра подібності, а так само сигналів, що надходять із вхідного й інтерфейсного шарів елементів.

Якщо отриманий параметр подібності задовольняє заданому параметру подібності, то пропоноване зображення класифікується, щодо виділених класів при навчанні, відбувається коректування ваги зв'язків. Якщо ж параметр подібності не задовольняє заданому параметру, то поточний нейрон-переможець загальмовується й починається пошук іншого нейрона-переможця з нейронів, що залишилися, розпізнавального шару Y. При ситуації, коли всі нейрони шару, що розпізнає, загальмовані, виділяється новий клас зображення й коректуються ваги зв'язків.

Для подальшого розпізнавання вхідних образів змодельована надбудова над верхнім розпізнавальним шаром нейронів. Вона являє з себе матрицю відповідностей, на горизонталі якої розташовані номери зображень, а по вертикалі – номера нейронів-переможців. У процесі розпізнавання, знаючи номер Y-нейрона, що спрацював, можна одержати весь список подібних вхідному еталонних зображень. Ця програмна надбудова полегшує процес аналізу, надає людині, якщо це буде необхідно, пояснення того, чому було прийняте те чи інше рішення.

При опису алгоритму використалися наступні позначення: m – максимальне число елементів, що розпізнають; n – число компонентів у вхідному векторі; Sk – n-мірний бінарний вхідний вектор, k = 1, …, q; q – число вхідних векторів; UвихS = (UвихS1, …, UвихSm) – вхідний шар; UвихZ = (UвихZ1, …, UвихZn) – інтерфейсний шар; UвихY = (UвихY1, …, UвихYm) – шар, що розпізнає; ||X|| - норма вектору X; ||Z|| – норма вектору Z; P – заданий параметр подібності, 0<p<1; Psh – отриманий параметр подібності; W1ij – вага зв'язку від елемента Zi (i = 1, …, n) до елемента Yj (j = 1, …, m); W2ji – вага зв'язку від елемента Yj до елемента Zi (j = 1, …, m; i = 1, …, n); L – константа, що перевершує одиницю.

Представимо алгоритм навчання мережі АРТ-1 крок за кроком.

Крок 1. Ініціалізація параметрів, завдання початкових значень: n, m, L, p, вагів зв'язків Wij1 та Wji2, шарів вхідного, інтерфейсного та розпізнавального Wij1 = 1/(1+ n); Wji2 = 1, (UвихSi = Sik , UвихZi = 0, де i = l, ..., n).

Крок 2. Поки не виконуються умови завершення, виконуються кроки 3 – 14 алгоритму навчання нейронної мережі.

Крок 3. Для кожного вхідного зображення Sk (k = 1, .., q) виконуються кроки 4 – 14.

Крок 4. Задаються нульові вхідні сигнали віх елементів, що розпізнають, у шарі Y; UвихYj = 0, j=1, ..., m.

Крок 5. Обчислюється норма вектору вихідних сигналів нейронів вхідного шару:

$$|| \text{UвихS} || = ||\text{Sk}|| = || U_{\text{вихS}} || = ||S^k|| = \sum_{i=1}^{n} S_i^{\,k} .$$

Крок 6. Формуються вхідні й вихідні сигнали елементів інтерфейсного шару: UвхZi = UвихSi, i =1, …, n; UвихZi = UвхZi , i =1, …, n.

Крок 7. Для кожного не загальмованого Y-нейрона (UвихYj $\neq$ -1) розраховується його вихідний сигнал:

$$\text{UвихYj} = U_{\text{вихYj}} = \sum_{i=1}^{n} W_{ij}^{\,1} \cdot U_{\text{вихZi}},\ j = 1, \ldots, m.$$

Крок 8. Поки не знайдено Y-нейрон, ваговий вектор якого відповідно до заданого значення параметра подібності P відповідає вхідному вектору Sk, виконуються кроки 9 - 12.

Крок 9. У шарі Y-нейронів визначається нейрон YJ, що задовольняє умові: UвихYJ ≥ UвихYj, j=1, .., m.

Якщо таких елементів декілька, те вибирається елемент із найменшим індексом. Якщо всі елементи розпізнавального шару UвихYJ = – l загальмовані, вважається, що вхідне зображення не може бути класифіковане.

Крок 10. Розраховуються вихідні сигнали Z-елементів: UвихZi = UвихSi WJi2, i = 1, …, n.

Крок 11. Обчислюється норма вектору вихідних сигналів інтерфейсного шарую:

$$\| \text{UвихZ} \| \| \text{U}_{\text{вихZ}} \| = \sum_{i=1}^{n} \text{U}_{\text{вихZi}}.$$

Крок 12. Обчислюється параметр подібності Psh: Psh = ||UвихZ|| / ||Sk||.

Якщо Psh < P, тобто умова не виконується, елемент YJ загальмовується (UвихYJ = – l), здійснюється перехід до кроку 8 алгоритму навчання нейронної мережі.

Якщо Psh ≥ P та умова можливості навчання нейрона YJ виконується, тоді здійснюється перехід до наступного кроку алгоритму.

Крок 13. Адаптуються ваги зв'язків елемента YJ. Wij1 = (LUвихZi)/(L-1+||UвихZ||), i=1,…,n;

WJi2=UвихZ, i=1, ..., n.

Крок 14. Перевіряються умови завершення. Умовами завершення роботи можуть бути: відсутність змін ваг Wij1 Wji2 , якщо протягом інтервалу або досягнення заданого числа.

Крок 15. Завершення роботи.

Засоби компенсації недоліків нейронної мережі АРТ-1. Для усунення недоліків роботи нейронної мережі в роботі було зроблене наступне:

- для розв'язання проблеми порушення динамічності системи прийнято рішення побудови моделі нейронної мережі з комбінуванням динамічних і статичних масивів. Динамічні масиви дозволять розширювати мережу на скільки це буде необхідним. Границю розширенню нейронній мережі ставить лише обсяг оперативної пам'яті комп'ютера.

– для розв'язання проблеми можливого невірного розпізнавання образів, коли при незначній зміні параметрів двійковий вектор отримує дуже значні зміни, які відбиваються на результаті розпізнавання, прийнято особливі правила кодування вхідних параметрів. При обраних правилах кодування близькі по своїй суті значення вхідних параметрів мають близькі по двійковій структурі коди.

– для спостереження за процесом прийняття рішення нейронною мережею, до класичної структури мережі додано спеціальні масиви, що динамічно розширюються. У цих масивах зберігається вся історія векторів, що були пов'язані з кожний нейроном мережі. Аналіз цієї інформації дозволяє зробити висновок чому саме мережа прийняла те чи інше рішення. Також ця інформація дозволяє зробити швидке перенавчання окремо взятого нейрона з виключенням помилково розпізнаного вектору (такі дії називаються "відкатом системи").

Удосконалена структура нейронної мережі зображена на рис. 3.

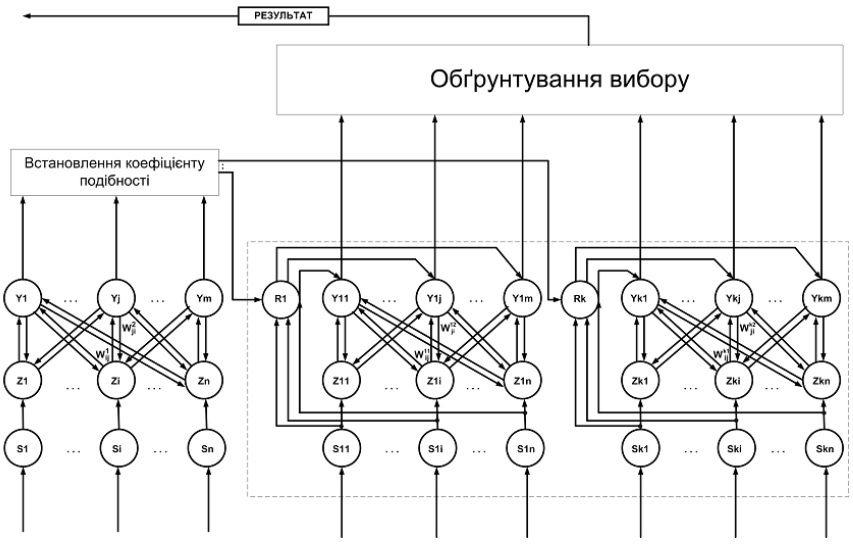

Рис. 3 – Модифікована структура мережі АРТ-1

Для поліпшення якості розпізнавання образів розроблену спеціальну систему нейронних мереж. Для кожної сторінки WEB-додатку, що захищається, відводиться одна нейронна мережа, яка несе в собі інформацію про всі легітимні дії з цією сторінкою. Нейронна мережа, що захищає окремо

взяту сторінку, має не тільки здатність запам'ятовувати легітимні дії користувача, але й відрізняти легітимні дії від нелегітимних. Окрім набору нейронних мереж, що захищають окремі сторінки WEB-додатку, існує це одна додаткова нейронна мережа, що відповідає за класифікацію користувачів. Класифікація користувачів потрібна для того, щоб встановлювати для нейронних мереж, що захищають сторінки WEB-додатку, параметра подібності відповідно до кожного класу користувача. Це потрібно для того, щоб нейронна мережа ставилася до дій "подозрілих" користувачів з більшою "увагою".

Таким чином стандартна структура нейронної мережі в процесі дослідження її недоліків, щодо розв'язання конкретної задачі, набула деяких нових рис. До нейронної мережі було додано спеціальні блоки для зберігання історії по кожному нейрону, а також було введено спеціальний механізм управління зміною параметра подібності для кожної мережі, що захищає окремо взяті сторінки WEB-додатку.

Після одержання результатів класифікації користувача (нейронна мережа зліва на рис. 3) та встановлення коефіцієнту подібності відповідно заданих правил, модифікуються коефіцієнти подібності для кожної з k нейронних мереж, що захищають сторінки WEB-додатку.

Якщо перша мережа, що відповідає за класифікацію користувачів не знайшла відповідного відбитку вектору, то вважається, що користувач раніше не робив ніяких дій, які могли викликати "підозру" у системи захисту. В такому випадку для нейронних мереж, що захищають сторінки WEB-додатку встановлюється деяке значення параметра подібності за замовчанням.

Коли мережа, що відповідає за класифікацію користувачів, знаходить у своїй пам'яті відбиток вектору подібний до вектору, що надійшов, то для нейронних мереж, що захищають сторінки WEB-додатку, встановлюється більш низький коефіцієнт подібності, тобто система буде ставитися до такого користувача більш ретельно, бо його дії раніше викликали підозру.

Нейронні мережі, що захищають сторінки WEB-додатку працюють за таким же принципом, як і нейронна мережа, що класифікує користувачів, але результати роботи першої інтерпретуються з точністю до навпаки. Коли нейронна мережа знайшла у своїй пам'яті відбиток вектору, що надійшов на входи, то поведінка користувача вважається нормальною, бо на початковому етапі нейронну мережу навчили поняттю "нормальної поведінки".

Якщо нейронна мережа, що захищає окремо взяту сторінку WEB-додатку, не знаходить відповідності вхідного вектору до збережених раніше векторів, то система починає стежити за таким користувачем. Якщо кількість дій, що визивають "занепокоєння" у системи перевищує деяке заздалегідь задане число, то система добавляє відбиток користувача до нейронної мережі класифікації користувачів з поміткою "підозрілий користувач". Останнє означає, що коефіцієнт подібності для такого користувача зменшується і якщо він у подальшому буде проводити "підозрілі" дії, то система класифікує його як зловмисника і блокує його доступу до WEB-додатку з видачою повідомлення адміністратору системи.

Адміністратор, проглянувши висновок системи і підтвердивши, що користувача було вірно класифіковано як зловмисника, тим самим навчає систему. Таким чином, чим більше часу працює система, тим більше інформації вона має.

Треба особливо зазначити, що система може цілком працювати без втручання адміністратора при відповідних налаштуваннях параметрів "лояльності" системи.

Результати досліджень. Нейронні мережі, які захищають окремі WEB сторінки сайту, працюють по аналогічному принципу, але результат їхньої роботи інтерпретується з точністю до навпаки: якщо була знайдена відповідність вхідного вектору в пам'яті мережі, то це нормальна ситуація, а якщо відповідності не було знайдено, то, можливо, ми маємо справу з атакою й необхідно більш пильно стежити за поточним користувачем.

Висновки. Запропонований метод побудови евристичної системи захисту WEB-додатків має істотні переваги порівняно з існуючим на сьогоднішній день методом детектування і відбиття атак на основі ModSecurity.

До переваг систем захисту на базі запропонованого методу можна віднести:

– здатність до виявлення нових типів атак, коли сигнатурний аналіз безсилий у силу своєї статичної природи;

– система не вимагає відновлення сигнатур, тому що засновано на аномаліях поведінки, тобто не потребує розробки і підтримки доволі не дешевої інфраструктури у мережі Internet, яка б дозволяла регулярно отримувати оновлення сигнатурних баз;

– дає можливість відслідковувати дії користувача, що неодноразово робить спроби проникнення, тобто "слідкує" за користувачем впродовж усіх циклів роботи з WEB-додатком;

– повністю адаптується під особливості WEB-додатку що захищає.

Як показали проведені експерименти, система здатна виявляти атаки, які не було виявлено на попередніх етапах сканування ні брандмауером, ні фільтром ModSecurity. При достатньому періоді навчання евристична система здатна виявляти до 40% таких атак.

Розроблений метод може застосовуватися як в якості додаткової ланки захисту у вже існуючих системах запобігання вторгнень, так і в якості самостійної системи виявлення та відбиття атак.

Список бібліографічного опису

1. Що таке VPN, і як ним безпечно користуватись. [Електронний ресурс]. Режим доступу: https://ukurier.gov.ua/uk/news/sho-take-vpn-i-yak-nim-bezpechno-koristuvatis/ t (дата звернення 17.10.2023).
2. PPP Protocol. [Електронний ресурс]. – Режим доступу: https://www.javatpoint.com/ppp-protocol (дата звернення 17.10.2023).
3. Value-Added Network (VAN): Definition, How It Works, and Purpose. [Електронний ресурс]. Режим доступу: https://www.investopedia.com/terms/v/value-added-network.asp (дата звернення 17.10.2023).
4. What Is a Network Access Server (NAS)? [Електронний ресурс]. Режим доступу: https://www.okta.com/identity-101/what-is-a-network-access-server/ (дата звернення 17.10.2023).
5. Web Application Firewall (ModSecurity). [Електронний ресурс]. Режим доступу: https://docs.plesk.com/en-US/obsidian/administrator-guide/server-administration/web-application-firewall-modsecurity.73383/# (дата звернення 17.10.2023).
6. Ken Coar, Rich Bowen. Apache Cookbook. [Електронний ресурс]. Режим доступу: https://www.oreilly.com/library/view/apache-cookbook/0596001916/ (дата звернення 17.10.2023).
7. І. А. Терейковський, Д. А. Бушуєв, Л. О. Терейковська. Штучні нейронні мережі: Базові положення. Навчальний посібник. Вид-во «Національний технічний університет України «КПІ», 2022 . с. 123.

References

1. What is a VPN and how to use it safely. [Electronic resource]. Access mode: https://ukurier.gov.ua/uk/news/sho-take-vpn-i-yak-nim-bezpechno-koristuvatis/ t (access date 10/17/2023).
2. PPP Protocol. [Electronic resource]. – Access mode: https://www.javatpoint.com/ppp-protocol (access date 10/17/2023).
3. Value-Added Network (VAN): Definition, How It Works, and Purpose. [Electronic resource]. Access mode: https://www.investopedia.com/terms/v/value-added-network.asp (access date 10/17/2023).
4. What Is a Network Access Server (NAS)? [Electronic resource]. Access mode: https://www.okta.com/identity-101/what-is-a-network-access-server/ (access date 10/17/2023).
5. Web Application Firewall (ModSecurity). [Electronic resource]. Access mode: https://docs.plesk.com/en-US/obsidian/administrator-guide/server-administration/web-application-firewall-modsecurity.73383/# (access date 10/17/2023).
6. Ken Coar, Rich Bowen. Apache Cookbook. [Electronic resource]. Access mode: https://www.oreilly.com/library/view/apache-cookbook/0596001916/ (access date 10/17/2023).
7. I. A. Tereykovskyi, D. A. Bushuev, L. O. Tereykovskaya. Artificial neural networks: Basic provisions. Tutorial. - Issued by "National Technical University of Ukraine "KPI", 2022 p. 123.