УДК 004.891

д.т.н., проф. **Лєнков С.В.** (ВІКНУ)
к.т.н., доц. **Джулій В.М.** (ХмНУ)
к.т.н. **Берназ Н.М.** (ДУТ)
Божук С.О. (ХмНУ)

АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ТА АЛГОРИТМІВ ВИЯВЛЕННЯ АТАК В БЕЗДРОТОВИХ МЕРЕЖАХ ПЕРЕДАЧІ ДАНИХ

Бездротові мережі передачі даних, у тому числі і локального типу, продовжують стрімко розвиватися, що пояснюється їх доступністю, простотою підключення користувачів і розповсюдженням мобільних пристроїв. Це обумовлено, в тому числі і збільшенням пропускної здатності безпровідних мереж. Однак бездротове середовище передачі даних в силу своїх особливостей створює потенційні умови для прослуховування мережевого трафіку і неконтрольованого підключення до бездротової мережі зловмисників, які знаходяться в зоні її дії. Дані мережі схильні, в тому числі з причини недосконалості протоколів, до різних типів атак. Для вирішення зазначених проблем забезпечення безпеки інформації в бездротових мережах використовуються як технічні засоби захисту, так і організаційні заходи.

Системи виявлення атак можуть бути реалізовані як на основі моделі виявлення відомих ознак (сигнатур), так і на основі виявлення відхилень від нормальної поведінки (аномалій). Бази даних містять тисячі сигнатур атак, їх використання підвищує вимоги до апаратного забезпечення і помітно уповільнює швидкість обробки мережевого трафіку, тому часто більшість правил адміністратор інформаційної безпеки відключає, що веде до підвищення ризику здійснення атаки. У свою чергу, технологія виявлення аномалій забезпечує захист від нових і невідомих вірусів і мережевих атак, але системи, побудовані на основі цього підходу, можуть видавати велику кількість помилкових попереджень, що веде до зниження чутливості до них.

Задача розробки алгоритмічного та програмного забезпечення системи, що дозволяє автоматизувати процес виявлення бездротових атак на основі застосування сучасних методів інтелектуального аналізу параметрів мережевого трафіку, є актуальною.

Широке розповсюдження бездротових локальних мереж та їх застосування в корпоративних інформаційних системах призводить до необхідності приділяти активну увагу вирішенню притаманних їм проблем інформаційної безпеки. При цьому існуючі засоби захисту, в тому числі комерційні бездротові системи виявлення атак, не забезпечують повноцінного захисту від зловмисної активності.

Для підвищення ефективності виявлення атак в бездротової локальної мережі організації необхідно розробити моделі і алгоритми розв'язування даної задачі на основі технологій інтелектуального аналізу даних.

Ключові слова: бездротові мережі, моделі, алгоритми, ефективність виявлення атак, метод, мережевий трафік, інформаційна безпека.

Вступ. Бездротові мережі передачі даних, у тому числі і локального типу, продовжують стрімко розвиватися, що пояснюється їх доступністю, простотою підключення користувачів і розповсюдженням мобільних пристроїв. Згідно з прогнозом компанії Cisco Systems, до 2017р. половина всього генерованого трафіку в корпоративних інформаційних мережах буде припадати на бездротові пристрої. Це обумовлено, в тому числі і збільшенням пропускної здатності безпровідних мереж. Однак бездротове середовище передачі даних в силу своїх особливостей створює потенційні умови для прослуховування мережевого трафіку і неконтрольованого підключення до бездротової мережі зловмисників, які знаходяться в зоні її дії. Дані мережі схильні, в тому числі з причини недосконалості протоколів, до різних типів атак. Рядові користувачі і невеликі організації, як правило, обмежуються використанням антивірусного програмного забезпечення, яке на сучасному етапі розвитку має ряд додаткових модулів захисту. Великі підприємства змушені купувати дорогі системи виявлення та запобігання атакам.

Для вирішення зазначених проблем забезпечення безпеки інформації в бездротових мережах використовуються як технічні засоби захисту, так і організаційні заходи. Технічні

засоби захисту по об'єкту застосування можна розділити на три основні групи: засоби захисту бездротової мережі в цілому; засоби захисту точки бездротового доступу; засоби захисту на стороні користувача (клієнта).

Постановка задачі. Системи виявлення атак можуть бути реалізовані як на основі моделі виявлення відомих ознак (сигнатур), так і на основі виявлення відхилень від нормальної поведінки (аномалій). Бази даних містять тисячі сигнатур атак, їх використання підвищує вимоги до апаратного забезпечення і помітно уповільнює швидкість обробки мережевого трафіку, тому часто більшість правил адміністратор інформаційної безпеки відключає, що веде до підвищення ризику здійснення атаки. У свою чергу, технологія виявлення аномалій забезпечує захист від нових і невідомих вірусів і мережевих атак, але системи, побудовані на основі цього підходу, можуть видавати велику кількість помилкових попереджень, що веде до зниження чутливості до них.

Задача розробки алгоритмічного та програмного забезпечення системи, що дозволяє автоматизувати процес виявлення бездротових атак на основі застосування сучасних методів інтелектуального аналізу параметрів мережевого трафіку, є актуальною.

Основна частина. Основу функціонування бездротової системи виявлення атак становить класифікаційна модель, на базі якої приймається рішення про віднесення фрагмента мережевого трафіку до нормальної активності або до будь-якого типу атаки. Формально завдання класифікації мережевого трафіку можна представити наступним чином (рис. 1), де X – множина вхідних образів (записів мережевої активності) x_i, Y – множина виходів (міток класів) y_i. Передбачається, що існує відображення $F: X \to Y$, значення якої відомі на записах кінцевої навчальної вибірки $X^m = \{(x_1, y_1),...,(x_m, y_m)\}$. Необхідно побудувати алгоритм $A: X \to Y$, здатний класифікувати довільну запис мережевої активності $x_i \in X$ (рис. 1).

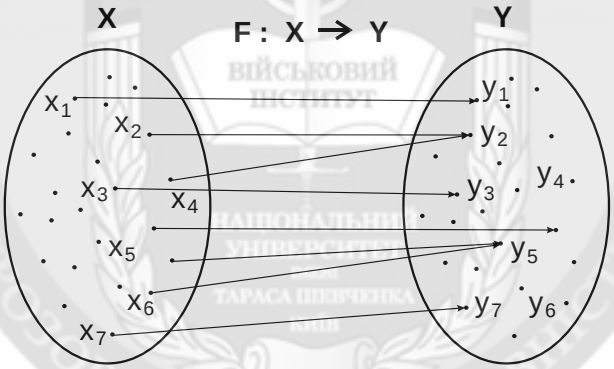

Рис. 1. Графічне представлення задачі класифікації мережевого трафіку

У загальному випадку можливі три результати процесу класифікації записів мережевої активності (рис. 2):

1. Правильне рішення: $S_0 \to H_0$ або $S_1 \to H_1$. Відповідно, ймовірність правильної класифікації записів визначається як:

$$P_{прав} = P\{H_0|S_0 \vee H_1|S_1\} = P\{H_0|S_0 + H_1|S_1\}. \quad (1)$$

2. Помилка першого роду: $S_0 \to H_1$. Ймовірність помилки першого роду:

$$P_1 = P\{H_1|S_0\}. \quad (2)$$

3. Помилка другого роду: $S_1 \to H_0$. Ймовірність помилки другого роду:

$$P_2 = P\{H_0|S_1\}. \quad (3)$$

Потрібно побудувати таку модель, яка дозволила б мінімізувати сумарну ймовірність виникнення помилок $P_{ВП} = P_1 + P_2$.

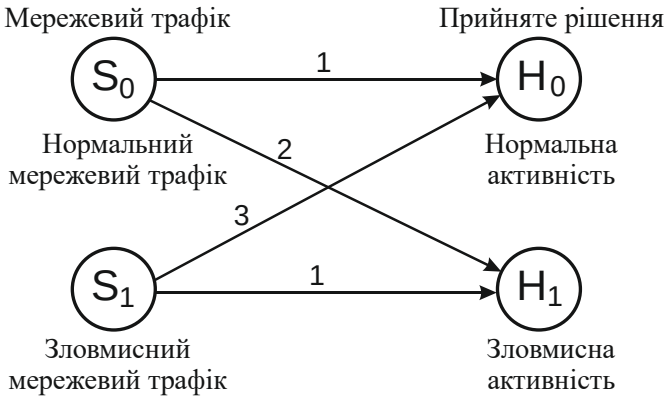

Рис. 2. Графічне представлення можливих результатів процесу класифікації

Для виявлення найбільш ефективного методу побудови класифікуючої моделі стосовно до бездротової системи виявлення атак проведемо порівняльний аналіз наступних методів: методу опорних векторів, метод *k*-найближчих сусідів, дерев прийняття рішень, а також нейронних мереж.

Метод опорних векторів за час свого існування показав як переваги по відношенню до раніше запропонованих методів, так і недоліки, які тим не менш, можуть бути подолані за рахунок більшої обчислювальної потужності комп'ютерного обладнання. Основу методу опорних векторів складає алгоритм класифікації, запропонований Вапніком. Головна ідея методу опорних векторів полягає в переведенні вхідних векторів в простір більш високої розмірності та пошук роздільної гіперплощини з максимальним зазором між кластерами в цьому просторі. По обидва боки гіперплощини, що розділяє різні класи, будуються дві паралельні гіперплощини (рис. 3). Роздільною гіперплощиною буде така гіперплощина, відстань від якої до двох паралельних гіперплощин максимальні. Цей алгоритм працює на припущенні, згідно з яким збільшення відстані між цими паралельними гіперплощинами призводить до зменшення середньої помилки класифікації.

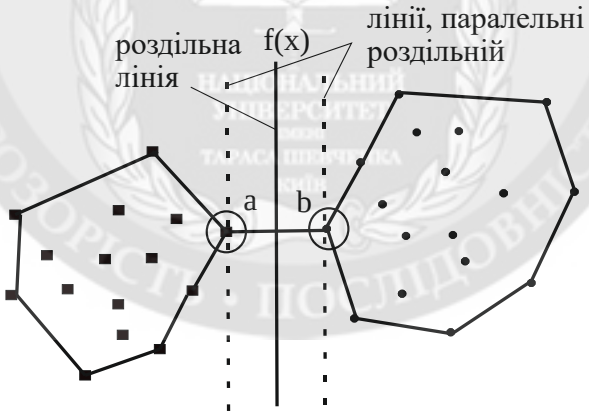

Рис. 3. Графічна інтерпретація методу опорних векторів
для двовимірного простору ознак

У випадку методу опорних векторів кожний об'єкт даних представлений у вигляді вектора в *n*-мірному просторі. Кожна точка належить лише одному з двох класів. Питання полягає в тому, чи можна розділити ці точки гіперплощиною з розмірністю ($n-1$). Таких гіперплощин, які класифікують дані, може бути безліч, вибирається така гіперплощина, відстань від якої до найближчої точки з навчального набору з кожної сторони гіперплощини максимально. Якщо дана гіперплощина існує, то вона є оптимальною роздільною гіперплощиною, а відповідний їй лінійний класифікатор – оптимально роздільним класифікатором. Найбільш близько розташовані вектори різних класів називаються опорними векторами (a і b на рис. 3). В якості переваг можна відзначити здатність до узагальнення, високу точність та низьку обчислювальну складність прийняття рішення. Недоліком даного

методу є відносно велика обчислювальна складність побудови класифікуючої моделі. Метод застосовувався для побудови класифікуючої моделі системи виявлення атак, що функціонує на основі технології сигнатурного аналізу, з даних навчальної вибірки.

Метод *k*-найближчих сусідів – метод класифікації, принцип роботи якого полягає у присвоєнні об'єкту класу, найбільш поширеного серед сусідів даного об'єкта. Формування сусідів відбувається з множиною об'єктів з уже відомими класами, і, виходячи з заданого значення k ($k \geq 1$), визначається, який з класів найбільш численний серед них. У разі якщо $k = 1$, то об'єкт просто відноситься до класу єдиного найближчого сусіда. Результати застосування методу легко піддаються інтерпретації. Недолік методу – його чутливість до локальної структури.

Дерева прийняття рішень являють собою деревоподібну структуру з «листя» і «гілок». На ребрах («гілках») дерева прийняття рішень записані атрибути, від яких залежить цільова функція, в «листі» записані значення цільової функції, а в інших вузлах – атрибути, за якими розрізняються об'єкти. Для класифікації нового об'єкта необхідно опуститися по дереву від кореня до листків та отримати відповідний клас. Таким чином, шлях від кореня до листка виступає правилами класифікації на основі значень атрибутів об'єкта. Перевагами дерев прийняття рішень є простий принцип їх побудови і хороша інтерпретованість результатів, недоліком – невисока точність класифікації.

Перераховані методи інтелектуального аналізу даних часто використовуються дослідниками в якості класифікаторів записів про мережеву активність.

Для вирішення практичних завдань, пов'язаних з розпізнаванням і класифікацією атак, активно застосовуються нейронні мережі. Нейронна мережа складається з взаємопов'язаних нейронів, що утворюють вхідний, проміжні (приховані) і вихідний шари. Навчання мережі відбувається шляхом коригування значень ваг нейронів для мінімізації помилки класифікації. Переваги нейронних мереж виражаються в їх здатності автоматично набувати знання в ході навчання, а також здатності до узагальнення, основний недолік полягає в чутливості до шуму у вхідних даних. Для підвищення швидкості обробки мережевого трафіку застосовується стиснення простору ознак з допомогою методу головних компонент і рециркуляційної нейронної мережі.

В даний час в області нейронних мереж бурхливо розвивається напрямок Deep Learning («глибоке навчання»), що представляє собою третє покоління нейронних мереж. У дану категорію входять багатошарові нейронні мережі, навчання яких здійснюється не на цілих об'єктах, а на їх складових частинах з поступовим збільшенням їх розміру. Прикладом є глибокі мережі довіри (Deep Belief Networks, DBN). В основі їх лежить RBM-мережа (Restricted Boltzmann Machine) – стохастична нейронна мережа, що складається з одного видимого і одного прихованого шарів, представлена на рис. 4.

Головною особливістю мереж глибокого навчання є процес навчання мережі, навчання проводиться пошарово без вчителя. Прихований шар RBM-підмережі виступає як видимий для наступної підмережі (рис. 5). По закінченні навчання можливе точне доналаштування DBN-мережі з учителем для функціонування в якості класифікатора.

Переваги мереж глибокого навчання: скорочення розмірності вектора даних (кількості ознак), що збільшує продуктивність при класифікації, і висока точність в задачах розпізнавання складних об'єктів (зображень, мови). Пропонується гібридна схема, яка об'єднує переваги глибоких мереж довіри і методу опорних векторів. На першому етапі використовується DBN-мережа для зменшення розмірності набору вхідних ознак, далі з допомогою SVM проводиться класифікація за чотирма категоріями мережевих атак і нормальної мережевої активності.

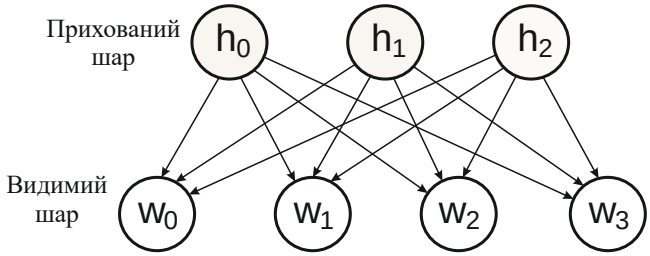

Рис. 4. Структура RBM-мережі

Наведені дослідження відносяться до виявлення вторгнень у традиційні провідні мережі. Проте роботи, присвячені безпосередньо застосуванню методів інтелектуального аналізу даних для розв'язання задачі виявлення атак, властивих локальним бездротовим мереж, відсутні.

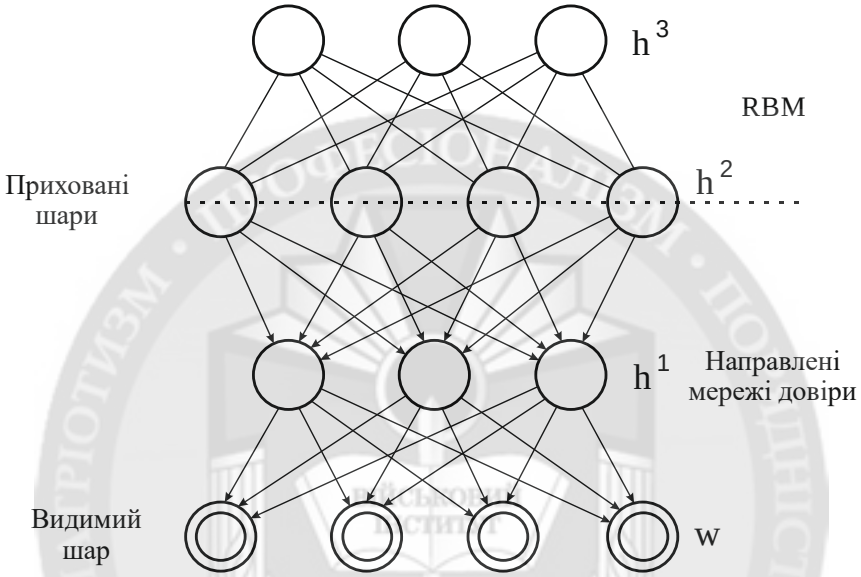

Рис. 5. Структура DBN-мережі

Існуючі системи виявлення вторгнень в бездротових мережах орієнтовані на аналіз протоколів бездротового зв'язку сімейства IEEE 802.11, ідентифікацію та аналіз підозрілої активності. Крім того, деякі виробники забезпечують можливість запобігання вторгнень в корпоративну мережу. У цьому випадку бездротові системи здатні здійснювати дії двох типів при виявленні атаки:

- бездротовий вплив – з'єднання між користувачем і точкою доступу обривається шляхом надсилання повідомлення про дисоціації (роз'єднання), після чого точка доступу відмовляє у відновленні з'єднання;

- мережевий вплив – система передає комутатору команду блокувати з'єднання з цим користувачем мережі по порту або MAC-адресою.

Крім того, деякі системи можуть визначити фізичне розташування джерела виявленої загрози з допомогою методу тріангуляції.

Основною перевагою системи WIPS компанії AirTight Networks є можливість її розгортання над існуючою мережевою інфраструктурою організації, тобто відсутня залежність від того, наскільки однорідна мережа організації. Рішення інтегрується з продукцією різних виробників мережевого устаткування. Також до переваг рішення варто віднести низьку вартість володіння і простоту установки.

Основні характеристики системи: автоматичне виявлення і блокування різних видів бездротових загроз, в тому числі несанкціонованих точок доступу і пасток, DoS-атак, Ad-Hoc мереж та ін; цілодобовий моніторинг продуктивності мережі; можливість функціонування сенсорів в режимі оффлайн; виявлення радіочастотного зашумлення і перешкод; розслідування бездротових інцидентів з журналів реєстрації; обчислення розташування

бездротового пристрою або джерела перешкод; захист мобільних пристроїв; інтеграція з платформами ArcSight, CheckPoint, McAfee ePO і Qualys, підтримка SNMP і Syslog; звіти про відповідність стандартів PCI DSS, SOX, HIPAA, GLBA, DoD Directive 8100.2; управління через фізичне підключення, віртуальний сервер або хмара.

В якості сенсорів використовуються власні пристрої AirTight C-75, C-60, C-55, C-50 з підтримкою одного або двох каналів і режимів роботи в ролі точки доступу або виділеного активного сенсора. Найбільш функціональні моделі мають підтримку стандарту 802.11ac і можливість підключення зовнішніх антен.

Ще однією популярною реалізацією WIDS для платформи Windows є AirMagnet Enterprise компанії Fluke Networks. Система дозволяє вирішувати наступні завдання: визначення несанкціонованих точок доступу і клієнтів; контроль політики безпеки використання бездротових мереж; виявлення атак в бездротовій мережі і протидія їм; локалізація зловмисника методом тріангуляції.

Основні характеристики AirMagnet Enterprise: підтримка стандарту 802.11ac; сигнатурний метод виявлення вторгнень для захисту більш ніж 230 загроз; наявність аналізатора радіочастот, що дозволяє виявляти перекриття каналів 802.11 і виявляти перешкоди; звіти про відповідність стандартам HIPAA, PCI DSS, GLBA, DoD, ISO 27001, BASEL 2 і CAD3; запобігання виявлених атак як за допомогою бездротового впливу, так і в кабельній мережі.

Перевагою системи є широкий набір ідентифікованих атак на канальний рівень бездротової мережі з їх докладним описом, гнучка система побудови звітів. Як суттєвий недолік системи можна виділити складність конфігурації, так як за замовчуванням настройки дозволяють використовувати тільки функціонал запобігання вторгнень. Для виявлення підроблених мереж і нелегальних точок доступу дана система вимагає значних налаштувань.

Система запобігання бездротових атак – Cisco Wireless Intrusion Prevention System (WIPS). Це бездротове рішення, яке дозволяє виявити і локалізувати як дротові, так і бездротові загрози на рівнях моделі OSI з фізичного до мережевого. Система виконує наступні функції: виявлення, класифікація та знешкодження помилкових пристроїв і неавторизованих мереж; моніторинг і усунення вразливостей; аналіз трафіку на предмет наявності слідів відомих утиліт для злому і поширених технологій атак; моніторинг і автоматична оптимізація продуктивності мережі; складання звітів з продуктивності і безпеки, в тому числі на відповідність стандартам.

Основні особливості Cisco WIPS: інтегрування функцій бездротового виявлення атак в об'єкти мережевої інфраструктури; розподілений аналіз трафіку та аномалій на точки доступу WLAN-контролерах; підтримка підключених до 3000 точок доступу; виявлення загроз і неполадок мережі в реальному часі; комбінування бездротового та дротового моніторингу трафіку, аналізу аномалій, перевірки характеристик і конфігурацій бездротових пристроїв; захист кадрів управління з допомогою протоколу Cisco MFP. У системі є можливість автоматизованого реагування на бездротові загрози як через бездротову мережу, так і методами, характерними для традиційних мереж.

Системи захисту від бездротових вторгнень дозволяють знаходити і нейтралізувати сторонні пристрої, захищати власних користувачів, контролювати і підтримувати на рівні продуктивність бездротових мереж і т. д. Разом з тим, хоча розглянуті WIDS пропонують ефективні способи виявлення вторгнень, вони мають і суттєві недоліки: неможливість виявлення невідомих типів бездротових атак і модифікацій наявних сигнатур атак; наявність характерних особливостей функціонування, за якими можна визначити конкретну модель системи і обійти її за відомою методикою; вразливість по відношенню до атак проти самих WIDS.

Крім цього, перераховані продукти мають відносно високу вартість, закритий вихідний код, а багато заявлених функції носять виключно рекламний характер.

Питання захищеності бездротових локальних мереж на даний момент залишаються відкритими. Основні проблеми захисту інформації в бездротових мережах укладаються при

цьому в наступному: поширення сигналу за межі контрольованої зони; легкий доступ зловмисника до бездротовому каналу передачі порівняно з кабельними мережами; використання вразливих протоколів і методів аутентифікації; відсутність повноцінного захисту від атак при випуску доповнень до стандартів; можливі помилки в налаштуванні різних компонентів бездротової мережі.

Для організації безпечного функціонування корпоративної бездротової мережі необхідно вибудувати систему багаторівневого захисту. Дана система включає в себе наступні рубежі (заходи): захист периметра бездротової мережі: точок доступу і пристроїв користувачів; забезпечення безпеки сеансів зв'язку: застосування надійних методів аутентифікації, стійких алгоритмів шифрування і т. д.; постійний моніторинг радіоефіру, включаючи фізичний рівень, виявлення і аналіз підозрілої активності.

Висновки. Широке розповсюдження бездротових локальних мереж та їх застосування в корпоративних інформаційних системах призводить до необхідності приділяти активну увагу вирішенню притаманних їм проблем інформаційної безпеки. При цьому існуючі засоби захисту, в тому числі комерційні бездротові системи виявлення атак, не забезпечують повноцінного захисту від зловмисної активності.

Для підвищення ефективності виявлення атак в бездротової локальної мережі організації необхідно розробити моделі і алгоритми розв'язування даної задачі на основі технологій інтелектуального аналізу даних.

ЛІТЕРАТУРА:

1. Васильев В.И. Интеллектуальные системы защиты информации: учеб. пособие / В. И. Васильев. – 2-е изд., испр. – М.: Машиностроение, 2012. – 171 с.

2. Гордейчик С.В. Безопасность беспроводных сетей. / С.В. Гордейчик, В.В. Дубровин – М.: Горячая линия – Телеком, 2008. – 288 с.

3. Гузаиров М.Б., Машкина И.В. Управление защитой информации на основе интеллектуальных технологий: учебное пособие. / М.Б. Гузаиров, И.В. Машкина– М.: Машиностроение, 2013. – 241 с.

4. Лєнков С.В. Концептуальна схема системи інтелектуальної обробки даних / С.В. Лєнков, В.М. Джулій, О.М. Горбатюк, Н.М. Берназ // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2014. – Вип. № 46. – С.181-190

5. Лукацкий А.В. Обнаружение атак. /А.В. Лукацкий – СПб.: БХВ-Петербург, 2003. – 608 с.

6. Таненбаум Э. Компьютерные сети. 5-е изд. / Э.Таненбаум, Д. Уэзеролл– СПб.: Питер, 2012. – 960 с.

REFERENCES:

1. Vasiliev V.I. Intellectual protection of information: Textbook. Allowance / V.I. Vasiliev. - 2 nd ed., Rev. - M .: Mechanical Engineering, 2012. - 171 p.

2. Gordeychik S.V. Safety of wireless networks. / S.V. Gordeychik, V.V. Dubrovin - M .: Hot line - Telecom, 2008. - 288 p.

3. Guzairov MB, Mashkina I.V. Managing the protection of information based on intelligent technology: a tutorial. M.B. Guzairov, I.V. Mashkin-M .: Mechanical Engineering, 2013. - 241 p.

4. S.V. Lyenkov A conceptual diagram of the data mining / SV Lyenkov, VM Julie, ON Gorbatyuk, NM Bernaz // Proceedings of the Military Institute of Taras Shevchenko National University of Kyiv. - K .: VIKNU 2014 - Vol. № 46. - p.181-190

5. Lukatsky A.V. Detection of attacks. / A.V. Lukatsky - St. Petersburg: BHV-Petersburg, 2003. - 608p.

6. Tanenbaum E. Computer networks. 5 th ed. / E. Tanenbaum, D. Wetherall- St. Petersburg: Peter, 2012. - 960 p.

Рецензент: д.т.н., проф. Сбітнєв А.І.

д.т.н., проф. Ленков С.В., к.т.н., доц. Джулий В.М., к.т.н. Берназ Н.М., Божук С.О.

АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ТА АЛГОРИТМІВ ВИЯВЛЕННЯ АТАК В БЕЗДРОТОВИХ МЕРЕЖАХ ПЕРЕДАЧІ ДАНИХ

Беспроводные сети передачи данных, в том числе и локального типа, продолжают стремительно развиваться, что объясняется их доступностью, простотой подключения пользователей и распространением мобильных устройств. Это обусловлено, в том числе и увеличением пропускной способности беспроводных сетей. Однако беспроводная среда передачи данных в силу своих особенностей создает потенциальные условия для прослушивания сетевого трафика и неконтролируемого подключения к беспроводной сети злоумышленников, которые находятся в зоне ее действия. Данные сети подвержены, в том числе по причине несовершенства протоколов, к различным типам атак. Для решения указанных проблем обеспечение безопасности информации в беспроводных сетях используются как технические средства защиты, так и организационные меры.

Системы обнаружения атак могут быть реализованы как на основе модели обнаружения известных признаков (сигнатур), так и на основе выявления отклонений от нормального поведения (аномалий). Базы данных содержат тысячи сигнатур атак, их использование повышает требования к аппаратному обеспечению и заметно замедляет скорость обработки сетевого трафика, поэтому часто большинство правил администратор информационной безопасности отключает, что ведет к повышению риска осуществления атаки. В свою очередь, технология выявления аномалий обеспечивает защиту от новых и неизвестных вирусов и сетевых атак, но системы, построенные на основе этого подхода, могут выдавать большое количество ошибочных предупреждений, что ведет к снижению чувствительности к ним.

Задача разработки алгоритмического и программного обеспечения системы, что позволяет автоматизировать процесс обнаружения беспроводных атак на основе применения современных методов интеллектуального анализа параметров сетевого трафика, является актуальной.

Широкое распространение беспроводных локальных сетей и их применение в корпоративных информационных системах приводит к необходимости уделять активное внимание разрешению присущих им проблем информационной безопасности. При этом существующие средства защиты, в том числе коммерческие беспроводные системы обнаружения атак, не обеспечивают полноценной защиты от злонамеренной активности.

Для повышения эффективности обнаружения атак в беспроводной локальной сети организации необходимо разработать модели и алгоритмы решения данной задачи на основе технологий интеллектуального анализа данных.

Ключевые слова: беспроводные сети, модели, алгоритмы, эффективность обнаружения атак, метод, сетевой трафик, информационная безопасность.

Prof. Lenkov S.V., Ph.D. Juliy V.N., Ph.D. Bernaz N.M., Bozhuk S.O.

ANALYSIS OF EXISTING METHODS AND ALGORITHMS OF ATTACK DETECTION IN WIRELESS DATA NETWORKS

Wireless data transmission networks, including local ones, continue to grow rapidly, which is explained by their availability, ease of connection of users and the proliferation of mobile devices. This is due, among other things, to the increase in the throughput of wireless networks. However, the wireless media environment, by virtue of its features, creates potential conditions for listening to network traffic and uncontrolled connection to a wireless network of intruders who are in the zone of its operation. These networks are vulnerable, including due to imperfections of protocols, to various types of attacks. To solve these problems, security of information in wireless networks is used both by technical means of protection and by organizational measures.

Attack detection systems can be implemented both on the basis of a model for detecting known signs (signatures) and on the basis of detecting deviations from normal behavior (anomalies). Databases contain thousands of attack signatures, their use increases hardware requirements and significantly slows down the processing speed of network traffic, so often the administrator of the information security rules off most of the rules, which leads to an increased risk of attack. In turn, anomaly detection technology provides protection against new and unknown viruses and network attacks, but systems based on this approach can produce a large number of erroneous warnings, which leads to a decrease in sensitivity to them.

The task of developing algorithmic and software systems, which makes it possible to automate the detection of wireless attacks based on the use of modern methods of intelligent analysis of network traffic parameters, is relevant.

The widespread use of wireless LANs and their use in corporate information systems makes it necessary to pay active attention to resolving inherent information security problems. At the same time, existing security measures, including commercial wireless intrusion detection systems, do not provide full protection against malicious activity.

To increase the efficiency of detecting attacks in an organization's wireless LAN, it is necessary to develop models and algorithms for solving this task based on data mining technologies.

Keywords: wireless networks, models, algorithms, effectiveness of attack detection, method, network traffic, information security.