УДК 004.056.21

д.т.н., проф. **Толюпа С.В.** (КНУ)
к.т.н., доц. **Плющ О.Г.** (ДУТ)
к.т.н., доц. **Пархоменко І.І.** (КНУ)

DOI: https://doi.org/10.17721/2519-481X/2020/68-09

ПОБУДОВА СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНУ МЕРЕЖУ НА ОСНОВІ МЕТОДІВ ІНТЕЛЕКТУАЛЬНОГО РОЗПОДІЛУ ДАНИХ

У статті запропонована комбінаторна побудова системи виявлення мережевих атак на основі вибраних методів інтелектуального аналізу даних та проведені експериментальні дослідження, що підтверджують ефективність створеної моделі виявлення для захисту розподіленої інформаційної мережі. Проведені експерименти з програмним прототипом показали високу якість виявлення мережевих атак і довели правильність вибору методів інтелектуального аналізу даних і застосовність вироблених методик.

Проаналізовано стан захищеності інформаційно-телекомунікаційних систем по протидії від кібератак, що дало можливість зробити висновки, що для забезпечення безпеки кіберпростору необхідне впровадження комплексу систем і механізмів захисту, а саме систем: розмежування доступу користувачів; міжмережного екранування; криптографічного захисту інформації; віртуальні приватні мережі; антивірусного захисту елементів ІТС; виявлення і запобігання вторгнень; автентифікації, авторизації і аудиту; попередження втрати даних; управління безпекою та подіями; управління захищеності.

Проведено аналіз публікацій вітчизняних та іноземних фахівців, в яких узагальнюється:

досвід побудови систем виявлення атак, їх недоліки та переваги; побудова систем виявлення атак та вторгнень на основі застосування інтелектуальних систем.

За результатами розгляду сформовано пропозиції щодо:

побудови систем виявлення мережевих атак на основі вибраних методів інтелектуального аналізу даних та проведені експериментальні дослідження, що підтверджують ефективність створеної моделі виявлення для захисту розподіленої інформаційної мережі.

Ключові слова: кіберпростір, атака, нейромережа, інформаційно-телекомунікаційна мережа, системи виявлення атак, методи інтелектуального аналізу даних, тренувальна база.

Вступ та аналіз останніх досліджень. Інтенсивний розвиток інформаційно-телекомунікаційних мереж (ІТС) та технологій всебічно впливає на всі сфери діяльності суспільства. Переважна кількість сучасних державних та приватних підприємств використовує ІТС для управління виробничими процесами, підтримки прийняття рішень, пошуку необхідних даних тощо. Це забезпечує їм низку переваг, пов'язаних з: підвищенням продуктивності праці і мобільності працівників; високою оперативністю доступу до інформації та послуг; можливостями віддаленого управління ресурсами і процесами тощо.

Низка нещодавно реалізованих кібератак, які завдали шкоди багатьом державним установам та приватним підприємствам і організаціям в 2017 році (Ощадбанк, Укргазбанк, Укрпошта, Укрзалізниця, Укренерго, ДТЕК, Київенерго, Київводоканал, Міжнародні аеропорти «Бориспіль» і «Київ», Rozetka, Київстар, Vodafone Україна, Lifecell, Київський метрополітен, телеканали СТБ і ICTV, Нова пошта, мережа магазинів «Епіцентр», автозаправки WOG і ТНК тощо [1]) показали неготовність та недосконалість їх власних систем безпеки до раніше невідомих вторгнень.

У 2020 році в Україні зафіксували близько 1 мільйон випадків кіберзагроз. Серед них - мережеві атаки, спроби мережевого сканування, спроби WEB-атак, фішинг, DDoS-атаки, поширення шкідливого програмного забезпечення. З метою попередження можливих атак, Національний координаційний центр кібербезпеки (НКЦК) посилив співпрацю з приватними компаніями. Вони передбачають обмін інформацією про кіберзагрози та інциденти в сфері кіберзахисту для оперативного інформування, реагування, попередження можливих атак і взаємодопомоги [2].

Масовані кібератаки ініціюють створення спеціальних технічних рішень, засобів та систем протидії. Для виявлення мережевих вторгнень використовуються сучасні методи [3-7], моделі [8, 9], засоби [10-12], ПЗ [13] і комплексні технічні рішення для систем виявлення та запобігання вторгнень [14,15], які можуть залишатись ефективними при появі нових або модифікованих видів кіберзагроз. Але на практиці при появі нових загроз та аномалій, породжених атакуючими діями з невстановленими або нечітко визначеними властивостями, зазначені засоби не завжди залишаються ефективними і вимагають тривалих часових ресурсів для їх відповідної адаптації. Тому, системи виявлення вторгнень (СВВ) повинні постійно досліджуватись і удосконалюватись для забезпечення неперервності в їх ефективному функціонуванні.

На сьогодні вирішення питань забезпечення безпеки в ІТС та управління станом їх захищеності описується в роботах вітчизняних та закордонних дослідників, а саме: Бурячка В.Л., Гнатюка С.О., Корченко О.Г., Кузнецова О.О., Субача І.Ю., Юдіна О.К., Бучика С.С., Євсеєва С.П., Дудикевича В.Б., Казмирчук С.В., T. Ptaceka, G. Elmasry, P. Albers, O. Camp та інших.

Слід зазначити, що одним із актуальних напрямів, який активно розвивається у сфері інформаційної безпеки є виявлення кібератак і запобігання вторгнень в ІТС з боку неавторизованої сторони (НАС). Також слід наголосити, що атаки на ІТС з кожним роком стають все досконалішими, глобальнішими та частішими.

Основна частина. На сьогоднішній день ІТС дозволяє вирішувати найбільш актуальні завдання: надання користувачам можливості обміну інформаційними повідомленнями різного типу (мова, відео, дані); швидке та якісне отримання необхідної інформації з будь-якого віддаленого джерела в мережі; автоматизацію процесів обробки, накопичення, зберігання великих обсягів інформації в мережі, самого процесу виробництва інформації.

Для забезпечення безпеки кіберпростору необхідне впровадження комплексу систем і механізмів захисту, а саме систем: розмежування доступу користувачів; міжмережного екранування; криптографічного захисту інформації; віртуальні приватні мережі; антивірусного захисту елементів ІТС; виявлення і запобігання вторгнень; автентифікації, авторизації і аудиту; попередження втрати даних; управління безпекою та подіями; управління захищеності.

Системи виявлення вторгнень є одним з ключових компонентів комплексу засобів захисту інформації. Всі існуючі промислові СВВ і наукові розробки мають ті чи інші недоліки: обмежений спектр виявляються атак або підтримуваної програмно-апаратної середовища, складність адміністрування або створення профілю, висока обчислювальна складність.

Системи виявлення атак (СВА) являють собою окремий клас програмних засобів (ПЗ), під яким розуміють програми, процедури, правила, а також, якщо передбачено, супутніх їм документації та даних, що відносяться до функціонування системи обробки інформації. Повна назва СВА – це системи виявлення і запобігання атак, так як саме в можливості автоматизованої протидії атакам полягає одна з основних переваг таких систем, у порівнянні, наприклад, із засобами, заснованими на людському факторі. Проте надалі буде використовуватися найбільш усталена назва - система виявлення атак. Використання СВА дозволяє вирішити цілий ряд завдань, що забезпечують досягнення цілей інформаційної безпеки [16].

Системи виявлення мережевих атак збирають інформацію з пакетів мережевого трафіку, системних журналів і показників функціонування системи. Традиційні системи виявлення мережевих атак будуються на сигнатурному підході: за допомогою набору правил або сигнатур, що формуються експертами і розміщені в базу вирішальних правил, описуються всі можливі сценарії і особливості атак. У цього підходу існує безліч відомих недоліків. За допомогою аналізу сигнатур неможливо виявити нові види атак, тому що база вирішальних правил не містить інформації про відповідну атаці. Процес аналізу сигнатур для розподілених атак є вкрай складним завданням. Крім того, бази вирішальних правил популярних систем

виявлення вторгнень практично є загальнодоступними, тому порушник може протестувати можливості приховування атаки [18-19].

Перераховані проблеми підходу пошуку сигнатур змушують фахівців шукати альтернативні шляхи для організації захисту від мережевих атак. Одним з популярних напрямків досліджень є застосування різних методів інтелектуального аналізу даних (ІАД) в системах виявлення мережевих атак. В основі даних методів лежить припущення, що вся легітимна активність в системі може бути представлена у вигляді математичної моделі [20-22].

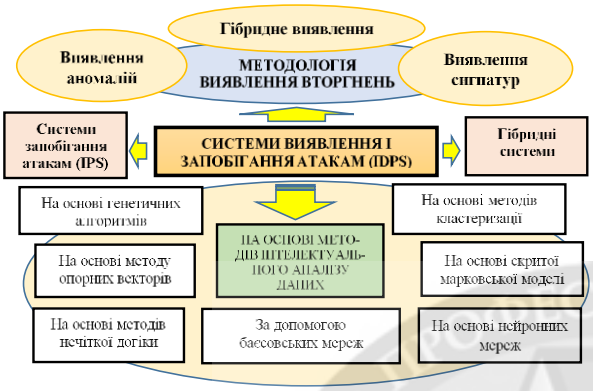

Рисунок 1 - Кваліфікаційні ознаки СВА на основі інтелектуальних методів аналізу даних

В останні десятиліття методи інтелектуального аналізу даних отримали широке застосування в багатьох наукових напрямах, і проблема виявлення мережевих атак не є винятком з цієї тенденції. Існують кілька сотень наукових досліджень щодо застосування різних методів інтелектуального аналізу даних для виявлення мережевих атак і для вирішення пов'язаних з виявленням підзадач.

Аналіз методів інтелектуального розподілу даних детально представлений в [23].

Описані в статті методики дозволяють використовувати всі вибрані методи інтелектуального аналізу даних для вирішення відповідних підзадач, пов'язаних з виявленням мережевих атак. У представлених методиках присутня значна кількість внутрішніх налаштувань. Для більшості налаштувань описані алгоритми по автоматичному вибору. Для інших видані рекомендації по ручному застосування при експериментальній побудові модулів виявлення для конкретних мережевих атак.

Рисунок 2 - Інтелектуальна система виявлення вторгнень

Звичайно протидіяти вторгненням і атакам основуючись тільки на одному з методів інтелектуального аналізу даних малоефективно, тому необхідно підійти до цього питання комплексно і побудувати інтелектуальну систему протидії вторгненням (рис. 2). При побудові такої інтелектуальної (експертної) системи пропонується вибрати нечітку модель. Це пов’язано з тим, що значна частина інформації про причини і джерела атак може бути отримана тільки експертним шляхом або у вигляді евристичних описів процесів. Для визначення джерел атак система безпеки має бути представлена моделлю тієї інформаційної мережі на яку вона орієнтується.

Данна модель ділить завдання переміщення інформації між комп’ютерами через середовище мережі на кількість рівнів менш великих і легше вирішуваних підзадач. Кожна з цих підзадач вирішується за допомогою одного рівня мережі. Тому первинне завдання для фахівця безпеки може бути представлене декомпозицією завдань безпеки по окремих рівнів мережі [24].

Аналіз останніх публікацій свідчить про те, що існуючі атаки, які застосовуються для проведення вторгнень в ІТС поділяються на 5 категорій. Кожна з категорій містить множину типів атак, які використовуються для реалізації мети вторгнення. В свою чергу кожен тип атаки несе загрозу мережі на відповідних рівнях мережевої моделі OSI та виконує свою функцію, щодо здійснення деструктивного впливу на мережу.

Серед лідерів детектування вразливостей можливо зазначити наступних розробників відповідних баз даних вразливостей: компанія MITRE та її база вразливосей Common Vulnerabilities and Exposures (CVE); National Institute of Standardsand Technology та база National Vulnerabilities Database (NVD); United State Computer Emergency Readiness Team та база Vulnerability Notes Database (VND), компанія IBM та база вразливостей X-Force та інші.

Питання вибору тренувальної бази з атаками не має простого рішення, тому що широко поширені бази даних містять багато в чому застарілі типи атак, а більш сучасні бази мають специфічну структуру, що вимагає складної попередньої обробки, і використовуються тільки окремими дослідниками, що перешкоджає порівнянні якісних показників результатів роботи.

При розробці та проведенні досліджень систем виявлення вторгнень однією з ключових завдань є вибір масивів даних, на яких буде проводитися тестування. Великі компанії-розробники в першу чергу орієнтуються на власні бази даних, спеціалізовані під конкретні завдання і область застосування.

На сьогоднішній день можна виділити дві найбільш поширені тренувальні бази даних з відомими атаками - DARPA і KDD.

Тренувальна база даних DARPA (Defense Advanced Research Project Agency) була сформована в рамках досліджень лабораторії Лінкольна Массачусетського технологічного інституту (MIT Lincoln Laboratory) в рамках дослідження можливостей різних систем виявлення вторгнень. Під час цього дослідження використовувалися дані мережевого трафіку і відомості від файлової системи для можливості ідентифікації змодельованих вторгнень, проведених фахівцями під час запису мережевих дампов. Тренувальні дані містять як реальний потік мережевого трафіку, так і спеціально змодельований фоновий трафік. Всі атаки були спрямовані на реальні обчислювальні системи.

В даний час тренувальні бази доступні всім дослідникам, тому значна частина публікацій у науковій літературі, пов'язаних з пропозицією нових методів і підходів з виявлення мережевих атак або аномалій, спираються на ці тестові дані. Використання даної бази даних дозволяє дослідникам по-рівняти основні характеристики якості виявлення: ймовірності помилок пропуску (false negative) і помилкового спрацьовування (false positive).

Загальна кількість типів атак, включених в тестові дані DARPA, склало 32 атаки. З точки зору атакуючого ці атаки можна розділити на чотири категорії: атаки відмови в обслуговуванні (Denial of Service, DoS); атаки переходу від віддаленого використання до локального (Remote to Local); атаки отримання користувачами прав суперкористувача (User to Root); атаки сканування або проб (Probing/surveillance).

Інформація про атаки DARPA зберігається у вигляді текстового опису, в якому вказується час початку атаки, тривалість, адреса жертви, назва атаки, категорія атаки та інші параметри.

На відміну від тренувальних даних DARPA, база даних KDD містить не дампи мережевого трафіку, а оброблені відомості у вигляді масивів з 42 ключових значень. Дана база успішно застосовується багатьма дослідниками для аналізу застосування різних математичних методів в завданні виявлення мережевих атак, в основному через можливість використання масивів даних з більшості програмних засобів без виконання додаткової обробки.

Зміст 42 параметрів, що розглядаються в базі даних KDD, був обґрунтований науково, присвяченими виявлення аномалій в мережевому трафіку. Однак при дослідженні можливостей по виявленню конкретних мережевих атак виявляється недостатньо аналізувати тільки представлені параметри, але також необхідно розглядати корисне навантаження мережевих пакетів - вищі рівні стека про-токолів TCP / IP. Крім позначених тренувальних баз даних існує безліч більш вузько спеціалізованих, але вони не набули такого широкого поширення в науковому середовищі.

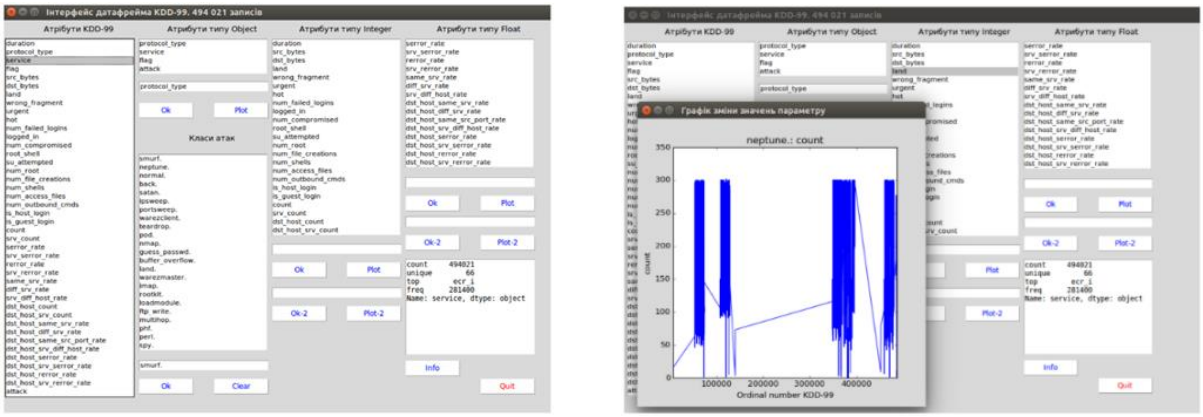

Рисунок 3 - Інтерфейс датафрейма KDD

Дослідниками пропонується безліч нестандартних рішень, що використовують конкретні особливості застосування даних методів. Формування СВВ на основі методів інтелектуального аналізу даних дозволяє позбутися від деяких відомих недоліків систем пошуку сигнатур і систем виявлення аномалій. Вибір конкретних методів і формування методик щодо застосування є складним завданням, що вимагає значних обсягів експериментів, і може сильно залежати від навчальної множини.

При розробці та проведенні досліджень систем виявлення вторгнень однією з ключових завдань є вибір масивів даних, на яких буде проводитися тестування. Великі компанії-розробники в першу чергу орієнтуються на власні бази даних, спеціалізовані під конкретні завдання і область застосування. Крім позначених тренувальних баз даних існує безліч більш вузько спеціалізованих, але вони не набули такого широкого поширення в науковому середовищі.

В рамках нашого дослідження були сформовані модулі виявлення для окремо взятих атак категорій User-to-Root і Remote-to-Local з тренувальних баз даних DARPA та KDD, які є найбільш складними для виявлення. Для більшості атак був отриманий результат в 100% правильно класифікованих пакетів. Для подібних атак отримані однакові набори «базових» параметрів. При об'єднанні кількох атак одного типу в класи також досягається 100% розпізнавання, при цьому збільшується кількість опорних векторів. Процес тестування складався з п'яти етапів. У першій частині тестування використовувалися багаторозрядні параметри трафіку, які добувають із заголовків IP і TCP пакетів. Всього використовувалося 14 базових параметрів, 6 для IP і 8 для TCP. Для значної частини атак було досягнуто 100% розпізнавання. На другому етапі, шляхом поділу багаторозрядних параметрів на кілька частин, кратних 8 бітам, число базових параметрів було збільшено до 24. В результаті аналогічного тестування для більшого числа атак було досягнуто 100% розпізнавання. У порівнянні з багаторозрядними параметрами збільшилася кількість опорних векторів, і велику роль став грати вибір даної матриці в методі головних компонент.

На третьому етапі тестування в набір розглянутих базових параметрів були включені статистичні параметри TCP-сеансів: час з'єднання, число переданих і прийнятих пакетів, байт і число пакетів з різними мітками - всього 49 базових параметрів. Для всіх розглянутих атак істотно збільшилася кількість опорних векторів в SVM-моделях, що викликано збільшенням розрядності простору. Для кількох атак так і не було отримано 100% результат. Для деяких атак виявилося досить від 2 до 5 нових параметрів з 49 для досягнення 100% розпізнавання та незначного збільшення числа опорних векторів. На четвертому етапі для атак, які не вдавалося виявити на попередніх етапах, була проведена кластеризація тренувальних даних і проведені процедури навчання нових модулів виявлення. В результаті майже для всіх розглянутих атак були побудовані кілька простих SVM-моделей, які дозволили класифікувати пакети зі 100% вірогідністю. Атаки, для яких не вдалося побудувати SVM-моделі, були проаналізовані та виявлено, що в складі тренувальних даних були присутні однакові пакети з різними мітками,

що призводило до неможливості побудови класифікатора. На п'ятому етапі було реалізовано розширення можливостей блоків кластеризації і класифікацій шляхом внесення нечіткості. В результаті побудовані пересічні кластери, однакові пакети з різними мітками були віднесені до класу атак з певною ймовірністю. Метод опорних векторів із застосуванням нечіткої логіки підвищив показники виявлення для окремих модулів. В результаті експериментального дослідження були отримані залежності числа опорних векторів від кількості нових параметрів для ряду атак. У всіх точках представлених залежностей досягнуто 100% розпізнавання. На на рис. 4 показані залежності при використанні тільки параметрів IP і TCP заголовків (всього 23 параметра).

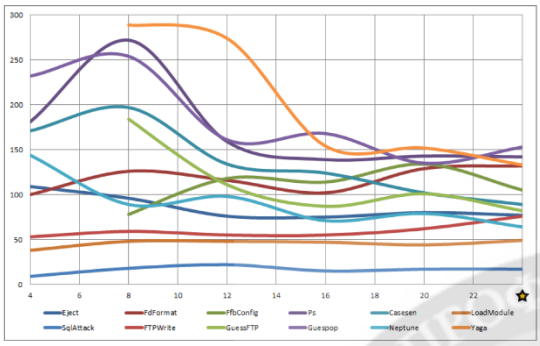

Рисунок 4 - Залежність числа опорних векторів від числа нових параметрів

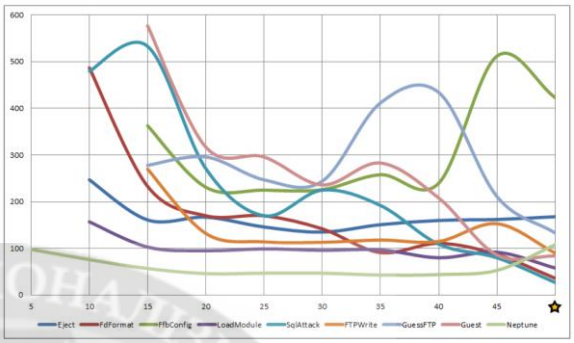

Рисунок 5 - Залежність числа опорних векторів від параметрів TCP-сеансів

На рис. 5 безліч параметрів доповнено параметрами TCP-сеансів (всього 49 параметрів). Зірочкою позначена робота без скорочення розмірності.

Для деяких атак, які не розпізнані програмним прототипом за допомогою одного модуля виявлення зі 100% ймовірністю, застосування декількох модулів виявлення з надмірною кількістю розглянутих «базових» і «нових» параметрів дозволяє скоротити число помилок другого роду до нуля. Проведені експерименти з окремими модулями виявлення показали хорошу працездатність системи та застосовність обраних інтелектуальних методів аналізу даних для поставленої мети. Метод опорних векторів дозволяє ідентифікувати значну частину розглянутих атак зі 100% ймовірністю, а в решті випадків помилка не перевищує декількох відсотків від числа всіх пакетів. Методи скорочення розмірності допомагають скоротити обсяг інформації, необхідної для класифікації мережевих пакетів й істотно підвищити продуктивність системи.

Проведене експериментальне дослідження підтвердило правильність запропонованої моделі та вибору безлічі методів інтелектуального розподілу даних, що лежать в її основі. Метод опорних векторів дозволив ідентифікувати більшість атак з результатом 98-100%. Метод головних компонент скоротив обсяг інформації, необхідної для класифікації мережевих пакетів, і підвищив швидкість формування модулів виявлення, але виявив проблему перенавчання. Методи кластеризації дозволили сформувати безліч модулів виявлення, виділивши типові фрагменти атак в окремі модулі виявлення та розбивши комплексні атаки на окремі модулі. Застосування нечіткої логіки підвищило результати роботи системи і дозволило класифікувати вектора, що мають різні мітки в навчальній вибірці.

На основі даного дослідження були детально опрацьовані сформульовані раніше методики по застосуванню методів інтелектуального розподілу даних по завданню виявлення мережевих атак [20]. Результати етапів експериментального дослідження наведені в таблиці 1.

Таблиця 1

Результати етапів експериментального дослідження

Метод анализу даних	Правильно розпізнано, %	Хибні сигнали, %
SVM (багаторозрядні параметри)	85	5
SVM	91	2
SVM + МГК	94	3
SVM + МГК + *k*-means	98	1
SVM + МГК + *k*-means + нечітка логіка	99	0,6

В табл. 2 представлені результати досліджень в сфері застосування методів інтелектуального розподілу даних в задачах виявлення мережевих атак.

Таблиця 2

Результати досліджень в сфері застосування методів інтелектуального розподілу даних в задачах виявлення мережевих атак

Метод анализа даних	Вірно розпізнано, %	Хибні сигнали, %
Quarter-sphere SVM	65	1
SVM	95,5	1
SVM + Генетичні алгоритми	99	-
SVM + Нечітка логіка	99,56	0,44
C4.5	95	1
C4.5 + МГК	92,16	-
C4.5 + Нейронні мережі	93,28	0,2
k-means кластеризація	65	1
Single leakage кластеризація	69	1
Y-means кластеризація	89,89	1
k-ближніх сусідів	92	1
Нейронні мережі + МГК	92,22	-
Багатошаровий персептрон	94,5	1
Генетичні алгоритми	97,47	0,69

Висновки. В статті запропоновано різні комбінаторні варіанти побудова системи виявлення мережевих атак на основі вибраних методів інтелектуального аналізу даних і проведені експериментальні дослідження, що підтверджують ефективність створеної моделі виявлення для захисту розподіленої інформаційної мережі.

Проведені експерименти показали високу якість виявлення мережевих атак і довели правильність вибору методів інтелектуального аналізу даних і застосовність вироблених методик. Застосування різних методів, можливість настройки внутрішніх параметрів і порогових значень дозволяють домогтися оптимального співвідношення продуктивності системи і точності розпізнавання атак в розподіленої мережі.

ЛІТЕРАТУРА:

1. Хакерські атаки на Україну [Електронний ресурс] // Вікіпедія : [сайт]. Київ, 2017. URL: https://is.gd/6lkWHY.

2. Хакерські атаки в Україні. [Електронний ресурс] // Вікіпедія : [сайт]. Київ, 2020. https://glavcom.ua/topics/ rosijskikhakeru.html.

3. Системы и методы обнаружения вторжений: современное состояние и направления совершенствования [Электронный ресурс] / А. А. Корниенко, И. М. Слюсаренко // CIT forum : [сайт]. 2009.

4. Аналіз систем та методів виявлення несанкціонованих вторгнень у комп'ютерні мережі [Електронний ресурс] / В. В. Литвинов [та ін.] // Математичні машини і системи. К : ІПММС НАН України, 2018. № 1. С. 31-40.

5. Анализ и классификация методов обнаружения сетевых атак / А. А. Браницкий, А. В. Котенко // Тр. СПИИРАН. 2016. № 2 (45). С. 207-244.

6. Сучасні методи виявлення аномалій в системах виявлення вторгнень / О.М. Колодчак // Вісник Національного ун-т «Львівська політехніка». Комп'ютерні системи та мережі. 2012. № 745. С. 98-104.

7. Дослідження методів виявлення вторгнень в телекомунікаційні системи та мережі / Д. О. Даниленко, О. А. Смірнов, Є. В. Мелешко // Системи озброєння і військова техніка. Х.: Харк. нац. ун-т Повітряних Сил ім. І. Кожедуба, 2012. № 1. С. 92-100.

8. The State of the Art in Intrusion Prevention and Detection [Electronic resourse] / Al-Sakib Khan Pathan. New York: Auerbach Publications, 2014.

9. Розробка моделі інтелектуального розпізнавання аномалій і кібератак з використанням логічних процедур, які базуються на покриттях матриць ознак / Г.Бекетова, Б. Ахметов, О. Корченко, В. Лахно // Безпека інформації. К: НАУ, 2016. Т. 22, № 3. С. 242-254.

10. Огляд систем виявлення атак в мережевому трафіку / К. М. Носенко, О. І. Півторак, Т. А. Ліхоузова // Адаптивні системи автоматичного управління. К: НТУУ КПІ, 2014. № 1 (24). С. 67-75.

11. Аналіз системи виявлення вторгнень та комп'ютерних атак / М. М. Радченко [та ін.] // Междисциплинарные исследования в науке и образовании. 2013. № 2.

12. Analysis of Host-Based and Network-Based Intrusion Detection System / Amrit Pal Singh, Manik Deep Singh. India: I. J. Computer Network and Information Security, 2014. Vol. 8. Pp. 41-47.

13. Аналіз сучасних систем виявлення атак і запобігання вторгненням / А. А.Завада, О. В. Самчишин, В. В. Охрімчук // Інформаційні системи. Житомир: Збірник наукових праць ЖВІ НАУ, 2012. Т. 6, № 12. С. 97-106.

14. An implementation of intrusion detection system using genetic algorithm / Mohammad Sazzadul Hoque, Md. Abdul Mukit, Md., Abu Naser Bikas // International Journal of Network Security & Its Applications (IJNSA). Sylhet, 2012. Vol. 4, No. 2. Pp. 109-120.

15. Analysis and Evaluation of Network-Based Intrusion Detectionand Prevention System in an Enterprise Network Using Snort Freeware / O. B. Lawal [et al.] // African Journal of Computing & ICT. Ibadan, 2013. Vol. 6, No. 2. Pp. 169-184.

17. IDS / IPS. Netgate Documentation: [website]. Washington: Rubicon Communications LLC, 2017. [Electronic resource]. Online: https://www.netgate. com/docs/pfsense/ids-ips/.

18. Довбешко С.В., Толюпа С.В., Шестак Я.В. Застосування методів інтелектуального аналізу даних для побудови систем виявлення атак. Науково-технічний журнал "Сучасний захист інформації". – №1. 2019. С. 56-62.

19. Toliupa S., Nakonechnyi V., Uspenskyi O. Signature and statistical analyzers in the cyber attack detection system. Information technology and security. Ukrainian research papers collection Volume 7, Issue 1 (12). С. 69-79.

20. Ghahramani, Z. An Introduction to hidden Markov models and Bayesian networks / Z. Ghahramani // International Journal of Pattern Recognition and Artificial Intelligence – 2001. –Vol. 15. – Pp. 9-42.

21. Barbara D. Detecting novel network intrusions using Bayes estimators / D. Barbara, J. Couto, S. Jajodia, N. Wu. // In: Proc. of the 1st SIAM International Conference on Data Mining. – 2001.

22. Kruegel, C. Bayesian event classification for intrusion detection / C. Kruegel, D. Mutz, W. Robertson, F. Valeur // In: Proc. of the 19th Annual Computer Security Applications Conference – 2003. – Pp. 14–23.

23. Толюпа С.В., Штаненко С.С., Берестовенко Г. Класифікаційні ознаки систем виявлення атак та напрямки їх побудови. Збірник наукових праць Військового інституту телекомунікацій та інформатизації імені Героїв Крут Випуск № 3. 2018р. С. 56-66.

24. Toliupa S.1, Druzhynin V.2, Parkhomenko I Signature and statistical analyzers in the cyber attack detection system. Scientific and Practical Cyber Security Journal (SPCSJ) № 3 (02) September 2018. Pp. 47-53.

25. Valdes, A. Adaptive model-based monitoring for cyber attack detection / A. Valdes, K. Skinner // In: Proc. of the Recent Advances in Intrusion Detection (Toulouse, France, 2000) – 2000. – Pp. 80-92.

26. Portnoy, L. Intrusion detection with unlabeled data using clustering / L. Portnoy, E. Eskin, S. J. Stolfo // In: Proc. of ACM Workshop on Data Mining Applied to Security. – 2001. – Pp. 1-14.

REFERENCES:

1. Hacker attacks on Ukraine [Electronic resource] // Wikipedia: [site]. Kyiv, 2017. URL: https://is.gd/6lkWHY.

2. Hacker attacks in Ukraine. [Electronic resource] // Wikipedia: [site]. Kyiv, 2020. https://glavcom.ua/topics/ rosijskikhakeru.html.

3. Systems and methods of detection of intrusions: the current state and directions of improvement [Electronic resource] / A.A. Kornienko, I.M. Slyusarenko // CIT forum: [site]. 2009.

4. Analysis of systems and methods for detecting unauthorized intrusions into computer networks [Electronic resource] / V.V. Litvinov [etc.] // Mathematical Machines and Systems. K: IPMMS NAS of Ukraine, 2018. № 1. Pp. 31-40.

5. Analysis and classification of methods for detecting network attacks / A.A. Branitsky, A.V. Kotenko // Tr. SPIIRAN. 2016. № 2 (45). Pp. 207-244.

6. Modern methods of detecting anomalies in intrusion detection systems / O.M. Kolodchak // Bulletin of the National University "Lviv Polytechnic". Computer systems and networks. 2012. № 745. pp. 98–104.

7. Research of methods of detection of intrusions into telecommunication systems and networks / D.O. Danilenko, O.A. Smirnov, E.V. Meleshko // Weapons systems and military equipment. H .: Hark. nat. University of the Air Force. I. Kozheduba, 2012. № 1. Pp. 92-100.

8. The State of the Art in Intrusion Prevention and Detection [Electronic resourse] / Al-Sakib Khan Pathan. New York: Auerbach Publications, 2014.

9. Development of a model of intelligent recognition of anomalies and cyberattacks using logical procedures based on the coverage of feature matrices / G. Beketova, B. Akhmetov, O. Korchenko, V. Lakhno // Information Security. K: NAU, 2016. T. 22, № 3. Pp. 242-254.

10. Review of attack detection systems in network traffic / K.M. Nosenko, O.I. Pivtorak, T.A. Likhouzova // Adaptive automatic control systems. K: NTUU KPI, 2014. № 1 (24). Pp. 67-75.

11. Analysis of the system of detection of intrusions and computer attacks / M.M. Radchenko [etc.] // Interdisciplinary research in science and education. 2013. № 2.

12. Analysis of Host-Based and Network-Based Intrusion Detection System / Amrit Pal Singh, Manik Deep Singh. India: I. J. Computer Network and Information Security, 2014. Vol. 8. Pp. 41-47.

13. Analysis of modern systems for detecting attacks and preventing invasion / A.A. Zavada, O.V. Samchyshyn, V.V. Okhrimchuk // Information systems. Zhytomyr: Collection of scientific works of ZhVI NAU, 2012. T. 6, №12. Pp. 97-106.

14. An implementation of intrusion detection system using genetic algorithm / Moham-mad Sazzadul Hoque, Md. Abdul Mukit, Md., Abu Naser Bikas // International Journal of Net-work Security & Its Applications (IJNSA). Sylhet, 2012. Vol. 4, no. 2. Pp. 109-120.

15. Analysis and Evaluation of Network-Based Intrusion Detectionand Prevention System in an Enterprise Network Using Snort Freeware / O. B. Lawal [et al.] // African Journal of Computing & ICT. Ibadan, 2013. Vol. 6, no. 2. Pp. 169-184.

17. IDS / IPS. Netgate Documentation: [website]. Washington: Rubicon Communications LLC, 2017. [Electronic resource]. Online: https: //www.netgate. com / docs / pfsense / ids-ips /.

18. Dovbeshko S.V., Toliupa S.V., Shestak Y.V. Application of data mining methods to build attack detection systems. Scientific and technical journal "Modern information protection". - №1. 2019. Pp. 56-62.

19. Toliupa S., Nakonechnyi V., Uspenskyi O. Signature and statistical analyzers in the cyber attack detection system. Information technology and security. Ukrainian research papers collection Volume 7, Issue 1 (12). with. 69-79.

20. Ghahramani, Z. An Introduction to hidden Markov models and Bayesian networks / Z. Ghahramani // International Journal of Pattern Recognition and Artificial Intelligence - 2001. - Vol. 15. - Pp. 9-42.

21. Barbara D. Detecting novel network intrusions using Bayes estimators / D. Barbara, J. Couto, S. Jajodia, N. Wu. // In: Proc. of the 1st SIAM International Conference on Data Min-ing. - 2001.

22. Kruegel, C. Bayesian event classification for intrusion detection / C. Kruegel, D. Mutz, W. Robertson, F. Valeur // In: Proc. of the 19th Annual Computer Security Applications Conference - 2003. - Pp. 14-23.

23. Toliupa S.V., Shtanenko S.S., Berestovenko G. Classification features of attack detection systems and directions of their construction. Collection of scientific works of the Military Institute of Telecommunications and Informatization named after Heroes of Kruty Issue № 3. 2018. with. Pp. 56-66.

24. Toliupa S.V., Druzhynin V.A., Parkhomenko I.I. Signature and statistical analyzers in the cyber attack detection system. Scientific and Practical Cyber Security Journal (SPCSJ) № 3 (02) September 2018. Pp. 47-53.

25. Valdes A. Adaptive model-based monitoring for cyber attack detection / A. Valdes, K. Skinner // In: Proc. of the Recent Advances in Intrusion Detection (Toulouse, France, 2000) - 2000. - Pp. 80-92.

26. Portnoy L. Intrusion detection with unlabeled data using clustering / L. Portnoy, E. Eskin, S. J. Stolfo // In: Proc. of ACM Workshop on Data Mining Applied to Security. - 2001. - Pp. 1-14.

Dr. Eng. Sc.Toliupa S., Ph.D. Pliushch O., Ph.D. Parhomenko I.

CONSTRUCTION OF SYSTEMS OF DETECTION OF INVASIONS INTO THE INFORMATI TON AND TELECOMMUNICATIONS NETWORK ON THE BASIS OF METHODS OF INTELLECTUAL DISTRIBUTION OF DATA

The article proposes a combinatorial construction of a network attack detection system based on selected methods of data mining and conducts experimental research that confirms the effectiveness of the created detection model to protect the distributed information network. Experiments with a software prototype showed the high quality of detection of network attacks and proved the correctness of the choice of methods of data mining and the applicability of the developed techniques.

The state of security of information and telecommunication systems against cyberattacks is analyzed, which allowed to draw conclusions that to ensure the security of cyberspace it is necessary to implement a set of systems and protection mechanisms, namely systems: delimitation of user access; firewall; cryptographic protection of information; virtual private networks; anti-virus protection of ITS elements; detection and prevention of intrusions; authentication, authorization and audit; data loss prevention; security and event management; security management.

An analysis of publications of domestic and foreign experts, which summarizes:

experience in building attack detection systems, their disadvantages and advantages;

construction of attack and intrusion detection systems based on the use of intelligent systems.

Based on the results of the review, proposals were formed on:

construction of network attack detection systems on the basis of selected methods of data mining and experimental research, which confirms the effectiveness of the created detection model for the protection of the distributed information network.

Keywords: cyberspace, attack, neural network, information and telecommunication network, attack detection systems, methods of data mining, training base.