УДК 004.67

О.С. САВЕНКО
Хмельницький національний університет

КРИТЕРІЇ КЛАСИФІКАЦІЇ МЕТОДІВ ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

В роботі проведено аналіз існуючих класифікацій методів виявлення шкідливого програмного забезпечення. Виокремлено критерії класифікації, зокрема характер отриманих даних, ознаки, що виступають об'єктом пошуку та дослідження, методи аналізу, алгоритми прийняття рішення, очікуваний результат та оцінка класифікації. На основі запропонованих критеріїв класифікації проведено класифікацію методів виявлення шкідливого програмного забезпечення.

Ключові слова: критерії класифікації, шкідливе програмне забезпечення, ознаки, поведінка.

O.S. SAVENKO
Khmelnytskyi National University

THE CLASSIFICATION CRITERIA FOR METHODS OF DETECTION MALICIOUS SOFTWARE

With the advent of a new malware, known antivirus products do not always confirm the declared level of authenticity of detection, because they are based on signature analysis. In contrast, to date, there are a large number of non-commercial tools based on new methods and approaches to detecting malware that are distinguished by the features used to identify SPS, the way data is received, and the methods of analysis. Therefore, in order to increase the efficiency and reliability of the detection of a new malware, the expedient task is to determine their characteristics that can be used in developing new detection methods, as well as the selection of criteria for classification of malware detection methods. An analysis of the existing classifications for methods of detecting malicious software is carried out. The classification criteria, in particular the character of the data received, the features serving as the object of search and research, the methods of analysis, decision-making algorithms, expected results of checking and assessment of classification, are singled out. On the basis of the proposed classification criteria, a classification for methods of detecting malicious software was conducted.

Keywords: classification criteria, malicious software, features, behaviour.

Вступ. Постановка задачі. На сьогоднішній день з стрімким поширенням комп'ютерних систем та інформаційних технологій, а також їхньої інтеграції у глобальну мережу Internet, шкідливе програмне забезпечення (malware) є одним із основних видів кіберзлочинності. Збитки, заподіяні шкідливим програмним забезпеченням (ШПЗ) при інфікуванні комп'ютерної системи чи мережі, можуть бути від незначного збільшення вихідного трафіку (якщо комп'ютер заражений троянською програмою, що надсилає спам) до повного порушення працездатності мережі або втрати критично важливих даних. Масштаб пошкоджень залежить від цілей вірусу, і іноді результати його діяльності непомітні для користувачів компрометованої комп'ютерної системи (КС) чи мережі. Так, наприклад, згідно із звітом компанії Cybersecurity ventures збитки, що завданні вірусами-вимагачами, зокрема вірусом WannaCry, у 2017 році склали близько 15 мільярдів доларів, що у 15 разів вище ніж у 2015 році [1].

З появою нового ШПЗ відомі антивірусні засоби не завжди підтверджують задекларований рівень достовірності виявлення, оскільки в їх основі лежить сигнатурний аналіз. На противагу їм на сьогоднішній день існує значна кількість некомерційних засобів, заснованих на нових методах та підходах до виявлення ШПЗ, що відрізняються ознаками, які використовуються для ідентифікації ШПЗ, способу отримання даних, методами аналізу.

Тому, з метою підвищення ефективності та достовірності виявлення нового ШПЗ, доцільним завданням є визначення їх характеристик, що можуть бути використанні при розробці нових методів виявлення, а також виокремлення критеріїв класифікації методів ШПЗ.

Основна частина. На сьогоднішній день існують різні підходи до класифікації методів виявлення ШПЗ. Загалом, всі методи виявлення ШПЗ можна розділити на два класи: методи виявлення відомого та нового ШПЗ [2]. Більш детальна класифікація запропоновано у роботі [3]. Класифікація була представлена з урахуванням наступних параметрів: дані, що отримані про досліджуване ПЗ, способи отримання цих даних, математичні методи, що застосовуються для аналізу даних та ознаки підозрілості, що характеризують ПЗ. Однак, запропонована класифікація не враховує очікуваний результат, що отримується в процесі виконання аналізу ШПЗ.

Інший однокритеріальний підхід до класифікації методів виявлення ШПЗ і систем виявлення вторгнень заснований на виборі методу машинного навчання: нейронні мережі, метод опорних векторів, байєсівські мережі, нечітка логіка, дерева прийняття рішень, тощо [4]. Проте, використання однокритеріального аналізу для проведення класифікації ШПЗ є неприйнятним, оскільки не враховується, які саме дані будуть використані в якості навчальної та тестової вибірки та яким чином було отримано ці дані.

З метою усунення недоліків відомих класифікації розроблено класифікацію методів виявлення ШПЗ, в основу якої закладено шість критерії: характер отриманих даних, ознаки, що виступають об'єктом пошуку та дослідження, методи аналізу, алгоритм прийняття рішень, очікуваний результат та оцінка класифікації (табл. 1). Розглянемо детально кожен критерій класифікації.

Характер отриманих даних. За характером отримуваних даних всі методи виявлення ШПЗ можна розподілити на сигнатурні та евристичні. Сигнатурні методи використовують пошук частин коду, що були характерними для визначеного типу вірусу чи іншого ШПЗ. Ці ділянки коду називаються сигнатурами вірусної програми (string pattern) і зберігаються в антивірусній базі даних. Така послідовність байтів повинна вибиратися з якомога менш схожими з рядками коду в довірених додатках чи інших типів вірусів.

Таблиця 1

Критерії класифікації

№ п/п	Назва критерію	Ознаки критерію
1	Алгоритм прийняття рішення	Експертна система, дерева рішень (алгоритм C4.5), приховані марківські моделі, найбільша спільна послідовність, метод опорних векторів, міра подібності косинус
2	Очікуваний результат	Точні та наближені методи
3	Ознаки, що виступають об'єктом пошуку та дослідження	Структурна інформація про файл, мережний трафік, множина операційних кодів, послідовності API викликів, граф потоку управління
4	Характер отриманих даних	Сигнатурні та евристичні методи
5	Методи аналізу	Динамічні та статичні методи
6	Оцінка класифікації	Вірність класифікації, точність, повнота, F-міра, крива помилок, AUC

Методи, що використовують набори правил (евристик), активізація яких, слугує припущенням про інфікування КС вірусною програмою називаються евристичними методами виявлення. Головною перевагою використання евристичних методів є здатність виявляти нові види вірусних програм. Окрім того, евристичні методи можуть не використовувати бази даних вірусних програм, що представлена сигнатурами вірусів.

Наприклад вірусні програми, в якості складових евристичних правил використовують елементи, які виражають деякі структурні особливості, що не притаманні корисним додаткам, а саме: наявність розриву між розділами, розташування виконуваного коду в останній секції коду, підозрілі характеристики розділу, підозріле ім'я секції (стандартними вважаються імена секцій .data, .code, .reloc, .idata, .text та ін.), невірне значення віртуального розміру в заголовку PE, використання декількох заголовків PE, підозрілі значення таблиці імпорту з бібліотеки KERNEL32.DLL, підозріле направлення коду [5]. Стосовно бот-мереж, наприклад, то евристичними складовими можуть бути: повторні DNS-запити до певного вузла мережі, високий вихідний SMTP-трафік, декілька КС в мережі, що виконують однакові DNS-запити, підозрілі вихідні повідомлення тощо [6].

Ознаки, що виступають об'єктом пошуку та дослідження. Відомі методи виявлення для ідентифікації різного виду ШПЗ використовують набори структурних особливостей виконуваних файлів, мережевого трафіку, вміст оперативної пам'яті, значення ключів системного реєстру, тощо. Фактично даний критерій визначає особливості (або ознаки), які вибираються для формування сигнатури або евристичних правил.

Методи аналізу. Важливою характеристикою методів виявлення ШПЗ є спосіб отримання даних про досліджуваний об'єкт. Всі методи аналізу можна розділити на дві групи: статичні та динамічні. Статичні методи аналізу досліджують вихідний шкідливий код без його виконання на реальній чи віртуальній системі та включають в себе пошук та виокремлення поведінкових властивостей про виконуваний файл. Статичний аналіз передбачає використання наступних підходів: дослідження структури виконуваних файлів (наприклад інформацію про компіляцію виконуваного файлу, експортовані та імпортовані бібліотеки), вилучення рядків та повідомлень, що можуть ідентифікувати ШПЗ, дослідження відбитку ШПЗ (fingerprinting), що включає формування хешу, визначення ознак навколишнього виконання, рядків реєстру, тощо. Також, одним із найпоширеніших підходів статичного аналізу є дизасемблювання виконуваного файлу. Процес дизасемблювання передбачає виконання процедури реверс-інженерінгу та перетворення виконуваного файлу у низькорівневий набір інструкцій для пошуку закономірностей та зв'язків. Перевагами використання даного підходу є висока швидкість та низьке ресурсоспоживання (у порівнянні з динамічними методами аналізу). Проте, використання статичного аналізу не дозволяє в повній мірі здійснювати виявлення ШПЗ, що змінює власну структуру в процесі виконання.

На противагу статичним динамічні методи аналізу передбачають виконання досліджуваного виконуваного файлу з метою отримання знань про поведінку ШПЗ. Зазвичай, при використанні динамічних методів аналізу залучають віртуальні машини, "пісочниці" або ресурси, що представляють собою приманку для ШПЗ (honeypot). В процесі дослідження виконуваного файлу можуть бути виявлені атрибути, що проявляються при виконанні зокрема, створення файлів, ключів реєстру, відкриття/закриття системних портів, створення мютексів та ін.

Алгоритм прийняття рішень. Після отримання даних або ознак про ШПЗ наступним етапом є обробка цих даних з використанням алгоритмів прийняття рішень. Взагалі алгоритми прийняття рішень можна розділити на дві категорії: методи засновані на експертних знаннях та методи машинного навчання.

Методи, що засновані на експертних знаннях використовуються для формалізації знань про ШПЗ та знань спеціалістів в області кібербезпеки. Система, що побудована на основі методів експертної оцінки, крім виконання обчислювальних операцій, формує висновки, що засновані на базі знань та продукційних правил. Знання можуть бути пов'язані наприклад, з тим, які дії є шкідливими (поведінковий аналіз), або які особливості структури свідчать про шкідливість виконуваного файл (структурний аналіз). Прикладами методів на основі експертної оцінки є метод продукційних правил, в основі яких закладено причинно-наслідкові зв'язки у вигляді конструкцій "Якщо-То"; нейромережні методи, тобто методи в основу яких закладено продукційні правил та нечіткий логічний висновок, що дозволяє визначати комплексні ознаки, в той час як елементи штучних нейронних мереж дозволяють адаптувати правила під відоме ШПЗ. Методи на основі експертної оцінки характеризуються високою достовірністю виявлення відомих зразків ШПЗ, проте вони є не досить ефективними

для ШПЗ, що застосовує нові техніки протидії антивірусному програмному забезпеченню.

Основна ідея будь-якої задачі машинного навчання полягає в тому, щоб навчити модель на основі алгоритму машинного навчання, для виконання завдань класифікації, кластеризації, регресії тощо. Навчання, що проводиться на основі вхідного набору даних і моделі, що будується, згодом використовується для прогнозування. Вихід такої моделі залежить від початкового завдання та реалізації. Одними із найпоширеніших алгоритмів машинного навчання для виявлення ШПЗ є: метод опорних векторів, C3.5, наївний баєсів класифікатор, дерева прийняття рішень, метод найближчого сусіда тощо.

Очікуваний результат. Метою здійснення задачі виявлення або ідентифікації ШПЗ є встановлення факту шкідливості програмного забезпечення. За ознакою результату, що формується після виконання процесу дослідження ШПЗ на предмет шкідливості, всі методи виявлення можна розділити на точні та наближені. Методи, що передбачають формування точного висновку, оперують бінарною множиною – шкідливе або не шкідливе програмне забезпечення. Як правило, точні методи дозволяють здійснювати виявлення визначеного класу ШПЗ або програмного забезпечення, що використовує тільки деякі із технологій, що використовуються для маскування або зміни шкідливого коду.

Наближені методи виявлення ШПЗ при визначені факту шкідливості використовують терміни нечіткої логіки, тобто при формуванні висновку можуть бути задіяні терміни висока, середня, низька підозрілість (шкідливість).

Оцінка класифікації. При розробці нових методів та алгоритмів виявлення ШПЗ, в результаті яких здійснюється віднесення досліджуваного об’єкта до одного із класів шкідливих чи корисних програм слід проводити оцінку класифікації. Процес оцінки класифікації заснований на використанні тестової вибірки, що складається з множини пар “набір характеристик – клас, що відповідає цим характеристикам”. При наявності тестової вибірки, перевірка роботи розробленого методу, зводиться до встановлення зв'язку його рішення з відомим правильним рішенням. Для того, щоб оцінити класифікацію використовуються чисельні показники його якості, найпоширенішими з яких є:

- Вірність класифікації (Accuracy). Визначає співвідношення кількості вірних рішень до загальної кількості розглянутих об’єктів:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

де TP – кількість вірно виявлених зразків ШПЗ, FN – кількість хибно класифікованих зразків ШПЗ, TN – кількість вірно ідентифікованих корисних програм, FP – є кількість корисних програм неправильно класифікованих як ШПЗ.

- Точність (Precision). Точність системи в межах класу визначається як частка об’єктів, що дійсно належать даному класу по відношенню до всіх об’єктів, які система віднесла до цього класу:

$$precision = \frac{TP}{TP + FP} \tag{2}$$

- Повнота (Recall). Часка знайдених класифікатором об’єктів, що належать класу відносно всіх документів цього класу в тестовій вибірці:

$$recall = \frac{TP}{TP + FN} \tag{3}$$

- F-міра. Оцінка, що визначає зважене гармонічне точності та повноти системи:

$$F_1 = \frac{2 precision \cdot recall}{precision + recall} \tag{4}$$

Крива помилок (ROC). Представлення результатів класифікації у вигляді залежності повноти та частки неправильно передбачених класів серед об'єктів негативного класу:

$$precision = TPR = \frac{TP}{TP + FN}, \qquad FPR = \frac{FP}{TN + FP} \tag{5}$$

- AUC. Кількісна інтерпретація кривої помилок, визначається як площа кривої, що обмежена ROC-кривою і віссю частки помилкових позитивних класифікацій.:

$$AUC = \int_0^1 TPR \, dFPR \tag{6}$$

Для здійснення дослідження методів виявлення ШПЗ, що представлене вірусними програмами, використаємо розроблену класифікацію (рис. 1). Розглянемо детальніше кожен з цих методів.

У роботі [7] запропоновано систему виявлення атак нульового дня, що працює в режимі реального часу та передбачає аналіз мережного трафіку. Запропонована система поєднує в собі використання трьох складових для виявлення ШПЗ: виявлення аномалій, сигнатурний та евристичний аналіз. Архітектура системи побудована з використанням трьох шарів, де кожен шар відповідає за одну складову та працює паралельно з усіма рештою. В якості алгоритму прийняття рішення застосовується метод опорних векторів.

Статичний підхід, що заснований на відстеженні API викликів представлено в роботі [8]. В якості наборів даних використовуються комбінація множин корисних додатків та ШПЗ. Кожен набір даних це API виклики, що отримуються з виконуваних файлів формату PE EXE з міткою класу, до якого вони належать. Для виконання класифікації застосовуються дерева прийняття рішень.

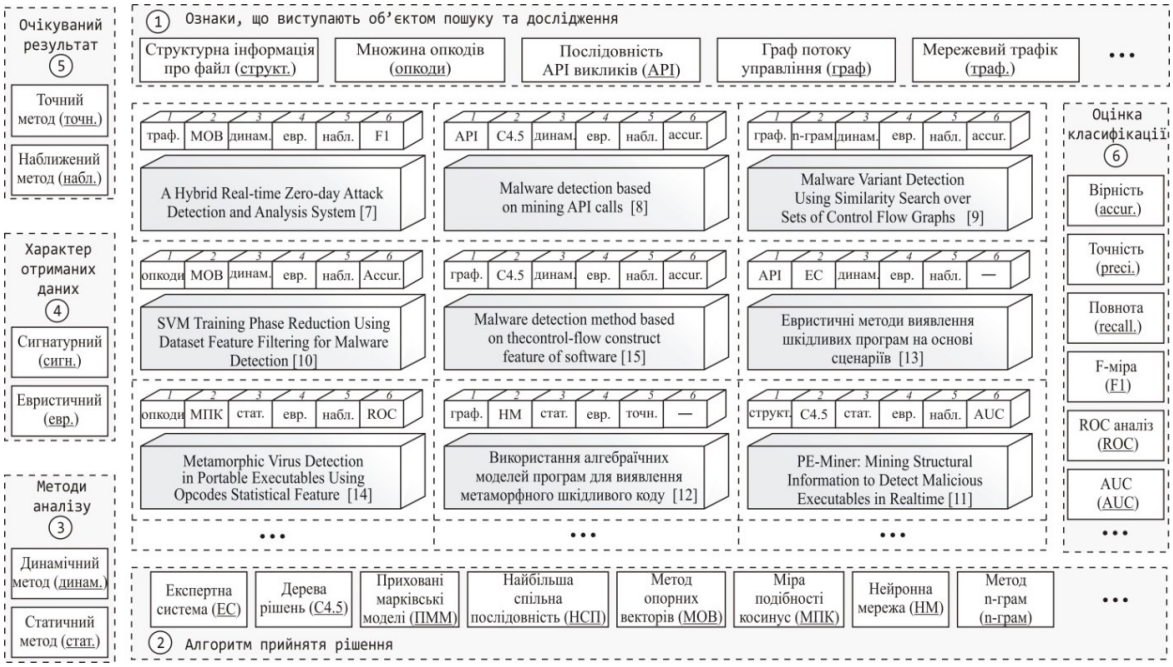

Рис. 1. Класифікація методів виявлення вірусних програм

Інший підхід для виявлення ШПЗ, зокрема поліморфних вірусів, полягає у представлені сигнатури вірусу у вигляді множини графів потоку керування (control flow graph) та пошуку подібності між ними [9]. Пошук схожості здійснюється на основі метрики відстані між векторами ознак, що представляються k-підграфами фіксованого розміру.

У роботі [10] автори здійснили аналіз щільності опкодів з використання методу опорних векторів. Для формування вектора ознак було використано віртуальне захищене середовище, в якому кожен тестовий зразок ШПЗ виконувався протягом трьох хвилин. З метою зменшення розмірності вектора ознак залучено метод головних компонент.

В [11] представлено метод, що базується на аналізі структури виконуваного файлу, зокрема секції заголовку представлено, для виявлення нового ШПЗ в режимі реального часу. В результаті дослідження було отримано 189 ознак для ідентифікації ШПЗ. Для здійснення класифікації було використано методи машинного навчання C3.5, наївний баєсів класифікатор та дерева прийняття рішень.

В роботі [12] представлено підхід для виявлення ШПЗ з метаморфним навантаженням на основі перевірки еквівалентності в алгебраїчних моделях послідовних програм та здійснюється оцінка стійкості деяких обфускуючих перетворень. Авторами теоретичним чином доводиться, що пошук еквівалентності для програм, які використовують техніки переключенням режиму і використанням зворотних операторів та їх комбінацій є мало ефективним та відносить задачу пошуку еквівалентності до класу NP повних задач.

Підхід, що заснований на побудові сценаріїв для виявлення ШПЗ представлено у роботі [13]. Запропоновані сценарії на основі API викликів, що здійснює програма, дозволяють представити поведінку шкідливих програм в ієрархічному вигляді Розроблено архітектуру евристика, що містить експертну систему на основі сценаріїв.

Представлені методи володіють рядом недоліків, які проявляються у високому рівні хибних спрацювань, спрощенням та наближенням тестових даних, орієнтацію на конкретні класи та технології, що використовує ШПЗ, що не дозволяє повністю вирішувати проблему виявлення нового ШПЗ, тощо. Тому, при розробці нових методів та підходів до виявлення ШПЗ доцільно враховувати недоліки відомих методів та використовувати комбіновані ознаки.

Висновок

В результаті виконання дослідження здійснено аналіз існуючих класифікацій методів виявлення шкідливого програмного забезпечення. З урахуванням недоліків відомих класифікації виокремлено критерії класифікації, зокрема характер отриманих даних, ознаки, що виступають об'єктом пошуку та дослідження, методи аналізу, алгоритми прийняття рішення, очікуваний результат та оцінка класифікації. На основі запропонованих критеріїв класифікації здійснено класифікацію методів виявлення шкідливого програмного забезпечення. Запропонована класифікація може бути використана при розробці нових методів та підходів для виявлення ШПЗ.

Література

1. Ransomware Damage Report. URL: https://cybersecurityventures.com/ ransomware-damage-report-2017-5-billion/. – Title from the screen.

2. Gandotra E. Malware Analysis and Classification: A Survey / E. Gandotra, D. Bansal, S. Sofat // Journal of Information Security. – 2014. – Vol. 5. – P. 56–64.

3. Подпружников Ю. Классификация методов обнаружения неизвестного вредоносного программного

обеспечения / Ю. Подпружников // Сборник трудов Современные тенденции технических наук. – 2011. – С. 22–25.

4. Singh J. A Survey on Machine Learning Techniques for Intrusion Detection Systems / J. Singh, M. J. Nene // International Journal of Advanced Research in Computer and Communication Engineering. – 2013. – Vol. 2, Issue 11. – P. 4349–4355.

5. Savenko O. Metamorphic Viruses' Detection Technique Based on the Equivalent Functional Block Search / O. Savenko, S. Lysenko, A. Nicheporuk, B. Savenko // CEUR-WS. – 2017. – Vol. 1844. – P. 555–569.

6. Pomorova O. A Technique for the Botnet Detection Based on DNS-Traffic Analysis / O. Pomorova, O. Savenko, S. Lysenko, A. Kryshchuk, K. Bobrovnikova // Computer Networks. – 2015. – Vol. 522. – P. 127–138.

7. Kelley R. A Hybrid Real-time Zero-day Attack Detectionand Analysis System / R. Kelley, M. Singh // International Journal Computer Network and Information Security. – 2015. – vol. 9. – P. 19–31.

8. Sami A. Malware detection based on mining API calls / A. Sami, B.Yadegari, H. Rahimi, N. Peiravian, S. Hashemi, A. Hamze // In Proc. of the 10th Symposium on Applied Computing. – 2010. – P. 1020–1025.

9. Cesare S. Malware Variant Detection Using Similarity Search over Sets of Control Flow Graphs / S. Cesare, Y. Xiang // In Proc. of the 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. – 2011. – P. 181–189.

10. O'Kane P. SVM Training Phase Reduction Using Dataset Feature Filtering for Malware Detection / P. O'Kane, S. Sezer, K. McLaughlin, E. G. Im // In Proc. of the 2013 IEEE Transactions on Information Forensics and Security. – 2013. – P. 500–509.

11. Shafiq M.Z. PE-Miner: Mining Structural Information to Detect Malicious Executables in Realtime / M.Z. Shafiq, S.M. Tabish, F. Mirza, M. Farooq // International Workshop on Recent Advances in Intrusion Detection. – 2009. – P.121–141.

12. Подловченко Р.И. Использование алгебраических моделей программ для обнаружения метаморфного вредоносного кода / Р.И. Подловченко, Н.Н. Кузюрин, В.С. Щербина, В.А. Захаров // Фундаментальная и прикладная математика. – М., 2009. – № 5. – С. 181–198.

13. Рувинская В.М. Эвристические методы детектирования вредоносных программ на основе сценариев / В.М. Рувинская, Е.Л. Беркович, А.А. Лотоцкий // Штучний інтелект. – 2008. – № 3. – С. 197–207.

14. Пат. на корисну модель 108238 Україна, МПК G06F 21/55. Мультиагентний спосіб локалізації бот-мереж у корпоративних комп'ютерних мережах / Поморова О.В., Савенко О.С., Крищук А.Ф., Лисенко С.М., Бобровнікова К.Ю., Нічепорук А.О. ; власник Хмельницький національний університет. – № u201600127 ; заявл. 04.01.2016 ; опубл. 11.07.2016, Бюл. № 13/2016.

15. Пат. на корисну модель 118456 Україна, МПК G06F 21/55. Спосіб виявлення метаморфних вірусів на основі статистичних метрик для визначення еквівалентних функціональних програмних блоків / Савенко О.С., Лисенко С.М., Бобровнікова К.Ю., Нічепорук А.О., Савенко Б.О. ; власник Хмельницький національний університет. – № u201701743 ; заявл. 23.02.2017 ; опубл. 10.08.2017, Бюл. № 15/2017.

References

1. Ransomware Damage Report. URL: https://cybersecurityventures.com/ ransomware-damage-report-2017-5-billion/. – Title from the screen.

2. Gandotra E. Malware Analysis and Classification: A Survey / E. Gandotra, D. Bansal, S. Sofat // Journal of Information Security, Vol. 5, 2014. – PP. 56-64.

3. Podpruzhnykov Yu. Klassyfykatsyia metodov obnaruzhenyia neyzvestnoho vredonosnoho prohrammnoho obespechenyia / Yu. Podpruzhnykov // Sbornyk trudov Sovremennye tendentsyy tekhnycheskykh nauk. – 2011. – S.22-25.

4. Singh J. A Survey on Machine Learning Techniques for Intrusion Detection Systems / J. Singh, M. J. Nene // International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 11, 2013. – PP. 4349-4355.

5. Savenko O. Metamorphic Viruses' Detection Technique Based on the Equivalent Functional Block Search / O. Savenko, S. Lysenko, A.Nicheporuk, B. Savenko // CEUR-WS, Vol. 1844. – 2017. – PP. 555-569.

6. Pomorova O. A Technique for the Botnet Detection Based on DNS-Traffic Analysis / O. Pomorova, O. Savenko, S. Lysenko, A. Kryshchuk, K. Bobrovnikova // Computer Networks, Vol. 522. – 2015. – PP. 127-138.

7. Kelley R. A Hybrid Real-time Zero-day Attack Detectionand Analysis System / R. Kelley, M.Singh // International Journal Computer Network and Information Security, vol. 9, 2015. – PP. 19-31.

8. Sami A. Malware detection based on mining API calls / A. Sami, B.Yadegari, H. Rahimi, N. Peiravian, S. Hashemi, A. Hamze // In Proc. of the 10th Symposium on Applied Computing. – 2010. – PP. 1020-1025.

9. Cesare S. Malware Variant Detection Using Similarity Search over Sets of Control Flow Graphs / S. Cesare, Y. Xiang // In Proc. of the 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. – 2011. – PP. 181-189.

10. O'Kane P. SVM Training Phase Reduction Using Dataset Feature Filtering for Malware Detection / P. O'Kane, S. Sezer, K. McLaughlin, E. G. Im // In Proc. of the 2013 IEEE Transactions on Information Forensics and Security. – 2013. – PP. 500-509.

11. Shafiq M.Z. PE-Miner: Mining Structural Information to Detect Malicious Executables in Realtime / M.Z. Shafiq, S.M. Tabish, F. Mirza, M. Farooq // International Workshop on Recent Advances in Intrusion Detection. – 2009. – PP.121-141.

12. Podlovchenko R.Y. Yspolzovanye alhebraycheskykh modelei prohramm dlia obnaruzhenyia metamorfnoho vredonosnoho koda / R.Y. Podlovchenko, N.N. Kuziuryn, V.S. Shcherbyna, V.A. Zakharov // Fundamentalnaia y prykladnaia matematyka. – M, 2009. – № 5. – S. 181-198.

13. Ruvynskaia V.M. Evrystycheskye metody detektyrovanyia vredonosnykh prohramm na osnove stsenaryev / V.M. Ruvynskaia, E.L. Berkovych, A.A. Lototskyi // Shtuchnyi intelekt. – 2008. – № 3. – S. 197-207.

14. Pat. na korysnu model 108238 Ukraina, MPK G06F 21/55 Multyahentnyi sposib lokalizatsii bot-merezh u korporatyvnykh kompiuternykh merezhakh / Pomorova O.V., Savenko O.S., Kryshchuk A.F., Lysenko S.M., Bobrovnikova K.Yu., Nicheporuk A.O.; vlasnyk Khmelnytskyi natsionalnyi universytet. – № u201600127; zaiavl. 04.01.2016; opubl. 11.07.2016, Biul. № 13/2016.

15. Pat. na korysnu model 118456 Ukraina, MPK G06F 21/55 Sposib vyiavlennia metamorfnykh virusiv na osnovi statystychnykh metryk dlia vyznachennia ekvivalentnykh funktsionalnykh prohramnykh blokiv / Savenko O.S., Lysenko S.M., Bobrovnikova K.Yu., Nicheporuk A.O., Savenko B.O.; vlasnyk Khmelnytskyi natsionalnyi universytet. – № u201701743; zaiavl. 23.02.2017; opubl. 10.08.2017, Biul. № 15/2017.

Рецензія/Peer review : 13.11.2017 р. Надрукована/Printed :25.01.2018 р.
Рецензент: стаття рецензована редакційною колегією