DOI 10.31891/2307-5732-2020-283-2-201-203
УДК 004.832.2

В.Ю. ТІТОВА, Ю.П. КЛЬОЦ, С.О. САВЧУК
Хмельницький національний університет

КЛАСИФІКАЦІЯ МОДЕЛЕЙ ЗАГРОЗ В КОМП'ЮТЕРНИХ СИСТЕМАХ

В даній статті розглянуто загрози комп'ютерним даним у комп'ютерних системах та проведено класифікацію зазначених загроз через їх характеристики. Взаємозв'язки між класами загроз та характеристиками становлять математичну модель задачі класифікації комп'ютерних загроз системою захисту комп'ютерних даних, наведену в даній статті. Аналіз побудованої моделі дозволяє зробити висновки, що задача класифікації комп'ютерних загроз належить до важко формалізованих задач та потребує для свого розв'язання не традиційних математичних методів, а методів інтелектуального аналізу, одним з яких можуть бути динамічні дерева рішень.

Ключові слова: *комп'ютерні загрози, математична модель, захист інформації, комп'ютерні системи.*

VERA YURIIVNA TITOVA, YURII PAVLOVYCH KLOTS, SERHII OLEHOVYCH SAVCHUK
Khmelnytskyi National University

CLASSIFICATION OF THREAT MODELS IN COMPUTER SYSTEMS

The article proposes an approach to the classification of threats in modern computer systems, which consists in determining the classes of potential threats and the set of characteristics that define these classes. The study found that the same characteristic in different circumstances, in particular in combination with other characteristics, may determine the different class of threats. Moreover, it should be borne in mind that at one point in time there may be both one and several classes of threats, and the characteristics may change in the decision-making process. And with their change, one threat class can move to another or correlate with it. The relationships between threat classes and their characteristics constitute a mathematical model of the threat classification problem by the computer data protection system. From the analysis of the mathematical model of computer threats classification it is possible to draw conclusions that the following features are inherent to the this problem: there are a large number of possible solutions, which requires a significant amount of time to solve the problem by a complete search of all available options. In addition, the input data can change in the process of solving the problem, and when changing at least one value, you need to go through all the available options first; input data is difficult to represent in the form of numerical data, and therefore the solution of the problem cannot be reduced to numerical calculations. Thus, the task of classifying threats to computer data is a difficult task. It is impractical to use traditional mathematical methods to solve it. Therefore, based on the features of the above problem to solve it, it is advisable to use methods of intellectual analysis, in particular dynamic decision trees.

Keywords: *computer threats, mathematical model, information protection, computer systems.*

Вступ. Однією з ключових сучасних проблем забезпечення комп'ютерної безпеки є необхідність ефективної протидії комп'ютерним загрозам. Причому треба враховувати, що загрози можуть бути як випадковими, так і навмисними. І найбільшу небезпеку становлять саме навмисні загрози. Крім того, обробка комп'ютерних даних здійснюється за допомогою різних складових комп'ютерної архітектури: апаратної, програмної, комплексної [1–4]. А тому актуальним завданням систем захисту комп'ютерних даних є захист усіх складових комп'ютерної архітектури від загроз як навмисних, так і випадкових.

Характеристика предметної області. На сьогоднішній день існує багато методів захисту комп'ютерних даних від загроз у комп'ютерних системах. Серед них можна виділити наступні [1–4]:

- методи виявлення аномалій – це методи знаходження та ідентифікації елементів, подій або спостережень, що не відповідають очікуваній поведінці (патернам) або іншим елементам набору даних;
- сигнатурні та евристичні методи виявлення шкідливого програмного забезпечення, засновані на порівнянні вмісту підозрілих програм та файлів з відомими зразками шкідливих програм;
- методи контролю доступу. Контроль доступу може здійснюватися по відношенню до користувача та по відношенню до даних. Найбільш розповсюджений контроль доступу користувача – це процедура реєстрації, при якій користувачеві необхідно ввести свій ідентифікатор та пароль. Система ж дозволить увійти лише тоді, коли його ідентифікатор співпаде з відомим системі і коли користувач знає пароль, пов'язаний з цим ідентифікатором. Контроль доступу, орієнтований на дані, полягає в тому, що кожному користувачеві може відповідати профіль, в якому вказуються дозволені операції і режими доступу до файлів.

Кожній групі методів притаманні як переваги, так і недоліки. Зокрема методи виявлення аномалій вимагають використання машинного навчання або засобів штучного інтелекту, що ускладнює їх програмно-апаратну реалізацію. Сигнатурні та евристичні методи можуть розпізнати атаку тільки у випадку, коли вона вже відома, тобто мала місце раніше. Методи контролю доступу потребують використання додаткових криптографічних протоколів, щоб унеможливити злам паролю та ідентифікатору, а також можуть створювати складнощі за необхідності спільного доступу до тих чи інших даних різним користувачам.

Використання зазначених методів в комплексі дозволило б нівелювати недоліки однієї групи через переваги інших та підвищити ефективність захисту комп'ютерних даних в цілому. Проте використання гібридної системи, в якій були б задіяні усі перелічені групи методів, могло б привести до падіння продуктивності комп'ютерної системи через високу потребу у ресурсах. А тому, більш доцільним вважається створення системи захисту, в якій та чи інша група методів буде задіюватися ситуаційно, залежно від типу виявленої загрози.

Постановка задачі. Отже, для того, щоб прийняти рішення про задіювання того чи іншого методу, система захисту комп'ютерних даних має містити підсистему, яка буде розв'язувати задачу класифікації комп'ютерних загроз. І саме реалізації зазначеної класифікації присвячено дану статтю.

Модель класифікації комп'ютерних загроз. Серед усієї множини загроз можна виділити наступні групи [5, 6]:

- загрози, що спрямовані на дані у пам'яті;
- загрози, пов'язані з коректністю вхідних даних;
- загрози, пов'язані з нестійкістю комп'ютерної системи;
- загрози, пов'язані з рівнем привілеїв та доступу;
- загрози, пов'язані з відмовою обслуговування, зокрема у роботі мережі;
- загрози, пов'язані з атаками на систему;
- загрози, пов'язані з апаратними складовими.

Математично, це можна записати наступним правилом:

$$Y_i =< Y_1, Y_2, Y_3, Y_4, Y_5, Y_6, Y_7 >,$$

де Y_1 – клас загроз, що спрямовані на дані у пам'яті; Y_2 – клас загроз, пов'язаних з коректністю вхідних даних; Y_3 – клас загроз, пов'язаних з нестійкістю комп'ютерної системи; Y_4 – клас загроз, пов'язаних з рівнем привілеїв та доступу; Y_5 – клас загроз, пов'язаних з відмовою обслуговування; Y_6 – клас загроз, пов'язаних з атаками на систему; Y_7 – клас загроз, пов'язаних з апаратними складовими; Y_i – клас поточної загрози.

Характеристики зазначених загроз можна представити у вигляді множини:

$$A = \{a_1, a_2, a_3, ..., a_{19}\},$$

де a_1 – переповнення буфера в зв'язку з неправильною роботою з даними; a_2 – висячий покажчик (посилання на об'єкт, що був видалений); a_3 – помилка форматного рядка; a_4 – маніпулювання метасимволами командної оболонки; a_5 – проникнення в запити; a_6 – відкритий доступ до системних областей; a_7 – маніпуляція з користувацькими скриптами; a_8 – гонки файлів у багатозадачних системах; a_9 – ескалація привілеїв; a_{10} – атака за допомогою символічних посилань; a_{11} – DOS-атака (проста або розподілена); a_{12} – підміна довіреного об'єкту мережі; a_{13} – нав'язування помилкового маршруту; a_{14} – аналіз мережного трафіку; a_{15} – сканування; a_{16} – неправильне конфігурування апаратних засобів; a_{17} – несанкціоноване використання закладок розробників; a_{18} – апаратне прослуховування середовища передачі даних; a_{19} – фізичний доступ до носіїв інформації.

При цьому, одна й та сама характеристика в різних обставинах, зокрема в комбінації з іншими характеристиками, може визначати собою різний клас загроз. Взаємозв'язки між характеристиками та класами загроз наведені в табл. 1.

Таблиця 1

Взаємозв'язок характеристик загроз з класами загроз

	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}	a_{17}	a_{18}	a_{19}
Y_1	+	+														+	+	+	
Y_2			+	+	+	+	+			+								+	
Y_3			+	+			+	+									+		
Y_4						+		+	+	+							+		
Y_5	+	+	+					+	+		+	+	+			+			+
Y_6				+	+	+	+			+	+	+	+	+	+		+	+	+
Y_7																+	+	+	+

Причому треба враховувати, що в один момент часу можуть мати місце як один, так і кілька класів загроз, а характеристики можуть змінюватися в процесі прийняття рішення. І з їх зміною один клас загрози може перейти в інший або корелювати з ним.

На основі проведеної класифікації можна побудувати математичну модель класифікації загроз системою захисту комп'ютерних даних (1).

З аналізу побудованої моделі класифікації комп'ютерних загроз можна зробити висновки, що даній задачі притаманні наступні особливості:

- наявна велика кількість можливих рішень, що потребує певних затрат часу для розв'язку задачі шляхом повного перебору усіх наявних варіантів. Крім того, вхідні дані можуть змінюватись у процесі розв'язку задачі, а при зміні хоча б одного значення необхідно перебирати усі наявні варіанти спочатку;
- вхідні дані важко представити у вигляді числових даних, а тому розв'язок задачі не може бути зведений до числових розрахунків.

Отже, задача класифікації загроз комп'ютерним даним належить до важко формалізованих задач [7]. Застосування для її розв'язку традиційних математичних методів є недоцільним. Тому, виходячи з особливостей вищевказаної задачі для її вирішення доцільно використати методи інтелектуального аналізу, зокрема динамічні дерева рішень.

$$Y_i = \begin{cases} Y_1, \text{якщо } A' = \{a_1, a_2, a_{16}, a_{17}, a_{18}\} \\ Y_2, \text{якщо } A' = \{a_3, a_4, a_5, a_6, a_7, a_{10}, a_{18}\} \\ Y_3, \text{якщо } A' = \{a_3, a_4, a_7, a_8, a_{17}\} \\ Y_4, \text{якщо } A' = \{a_6, a_8, a_9, a_{10}, a_{17}\} \\ Y_5, \text{якщо } A' = \{a_1, a_2, a_3, a_8, a_9, a_{11}, a_{12}, a_{13}, a_{16}, a_{19}\} \\ Y_6, \text{якщо } A' = \{a_4, a_5, a_6, a_7, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{17}, a_{18}, a_{19}\} \\ Y_7, \text{якщо } A' = \{a_{16}, a_{17}, a_{18}, a_{19}\} \\ Y_1 \cup Y_2, \text{якщо } A' = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_{10}, a_{16}, a_{17}, a_{18}\} \\ Y_1 \cup Y_3, \text{якщо } A' = \{a_1, a_2, a_3, a_4, a_7, a_8, a_{16}, a_{17}, a_{18}\} \\ Y_1 \cup Y_4, \text{якщо } A' = \{a_1, a_2, a_6, a_8, a_9, a_{10}, a_{16}, a_{17}, a_{18}\} \\ Y_1 \cup Y_5, \text{якщо } A' = \{a_1, a_2, a_3, a_8, a_9, a_{11}, a_{12}, a_{13}, a_{16}, a_{17}, a_{18}, a_{19}\} \\ Y_1 \cup Y_6, \text{якщо } A' = \{a_1, a_2, a_4, a_5, a_6, a_7, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{16}, a_{17}, a_{18}, a_{19}\} \\ Y_1 \cup Y_7, \text{якщо } A' = \{a_1, a_2, a_{16}, a_{17}, a_{18}, a_{19}\} \\ Y_2 \cup Y_3, \text{якщо } A' = \{a_3, a_4, a_5, a_6, a_7, a_8, a_{10}, a_{17}, a_{18}\} \\ Y_2 \cup Y_4, \text{якщо } A' = \{a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{17}, a_{18}\} \\ Y_2 \cup Y_5, \text{якщо } A' = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{11}, a_{12}, a_{13}, a_{16}, a_{18}, a_{19}\} \\ Y_2 \cup Y_6, \text{якщо } A' = \{a_3, a_4, a_5, a_6, a_7, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{17}, a_{18}, a_{19}\} \\ Y_2 \cup Y_7, \text{якщо } A' = \{a_3, a_4, a_5, a_6, a_7, a_{10}, a_{16}, a_{17}, a_{18}, a_{19}\} \\ Y_3 \cup Y_4, \text{якщо } A' = \{a_3, a_4, a_6, a_7, a_8, a_9, a_{10}, a_{17}\} \\ Y_3 \cup Y_5, \text{якщо } A' = \{a_1, a_2, a_3, a_4, a_7, a_8, a_9, a_{11}, a_{12}, a_{13}, a_{16}, a_{17}, a_{19}\} \\ Y_3 \cup Y_6, \text{якщо } A' = \{a_3, a_4, a_5, a_6, a_7, a_8, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{17}, a_{18}, a_{19}\} \\ Y_3 \cup Y_7, \text{якщо } A' = \{a_3, a_4, a_7, a_8, a_{16}, a_{17}, a_{18}, a_{19}\} \\ Y_4 \cup Y_5, \text{якщо } A' = \{a_1, a_2, a_3, a_6, a_8, a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{16}, a_{17}, a_{19}\} \\ Y_4 \cup Y_6, \text{якщо } A' = \{a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{17}, a_{18}, a_{19}\} \\ Y_4 \cup Y_7, \text{якщо } A' = \{a_6, a_8, a_9, a_{10}, a_{16}, a_{17}, a_{18}, a_{19}\} \\ Y_5 \cup Y_6, \text{якщо } A' = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{17}, a_{18}, a_{19}\} \\ Y_5 \cup Y_7, \text{якщо } A' = \{a_1, a_2, a_3, a_8, a_9, a_{11}, a_{12}, a_{13}, a_{16}, a_{17}, a_{18}, a_{19}\} \\ Y_6 \cup Y_7, \text{якщо } A' = \{a_4, a_5, a_6, a_7, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{17}, a_{18}, a_{19}\} \end{cases} \quad (1)$$

де A' – множина характеристик, що характеризують поточну загрозу.

Висновки

В статті було розглянуто загрози комп'ютерним даним у комп'ютерних системах та проведено їх класифікацію. На основі класифікації було запропоновано математичну модель визначення класу поточної загрози.

Зазначена модель є основою для створення підсистеми класифікації загроз системи захисту комп'ютерних даних, яка буде базуватися на методах інтелектуального аналізу, зокрема динамічних деревах рішень. Впровадження даної підсистеми підвищить ефективність системи захисту комп'ютерних даних та дозволить уникнути великих затрат у комп'ютерних ресурсах підчас функціонування зазначеної системи.

Література

1. Семененко, В.А. Информационная безопасность / В.А. Семененко. – М. : МГИУ, 2011. – 277 с. – ISBN 5-276-00872-8

2. Баранова Е.К. Информационная безопасность и защита информации : учеб. пособие / Е.К. Баранова, А.В. Бабаш. – М. : РИОР: ИНФРА-М, 2017. – 322 с. – ISBN: 978-5-369-01450-9

3. Нестеров С.А. Основы информационной безопасности / С.А. Нестеров. – М. : Изд. «Лань», 2016. – 324 с. – ISBN: 978-5-8114-2290-6

4. Бирюков А.А. Информационная безопасность. Защита и нападение / А.А. Бирюков. – М. : ДМКПресс, 2017. – 434 с. – ISBN: 978-5-97060-435-9

5. Корпань Я.В. Класифікація загроз інформаційній безпеці в комп'ютерних системах при віддаленій обробці даних / Я.В. Корпань // Мир науки и инноваций. – Иваново, Научный мир, 2015. – Т. 17, № 2. – С. 39–46.

6. Корпань Я.В. Комплекс методів і засобів захисту інформації у комп'ютерних системах / Я.В. Корпань // Реєстрація, зберігання і обробка даних. – 2015. – Вып. 1. – Т. 3 2. – С. 31–35.

7. Локазюк В. М. Засади систем підтримки прийняття рішень на основі комп'ютерних систем та їх компонентів : навч. посіб. / В. М. Локазюк, О. В. Іванов, В. Ю. Тітова ; Хмельниц. нац. ун-т. – Хмельницький : Гонта А.С., 2010. – 338 с.

References

1. Semenenko, V.A. Informacionnaya bezopasnost / V.A. Semenenko. – M. : MGIU, 2011. – 277 c. – ISBN 5-276-00872-8

2. Baranova E.K. Informacionnaya bezopasnost i zashita informacii : ucheb. posobie / E.K. Baranova, A.V. Babash. – M. : RIOR: INFRA-M, 2017. – 322 s. – ISBN: 978-5-369-01450-9

3. Nesterov S.A. Osnovy informacionnoj bezopasnosti / S.A. Nesterov. – M. : Izd. «Lan», 2016. – 324 s. – ISBN: 978-5-8114-2290-6

4. Biryukov A.A. Informacionnaya bezopasnost. Zashita i napadenie / A.A. Biryukov. – M. : DMKPress, 2017. – 434 s. – ISBN: 978-5-97060-435-9

5. Korpan Ya.V. Klasyfikatsiia zahroz informatsiinii bezpetsi v kompiuternykh systemakh pry viddalenii obrobtsi danykh / Ya.V. Korpan // Myr nauky y ynnovatsyi. – Yvanovo, Nauchnыi myr, 2015. – T. 17, № 2. – S. 39–46.

6. Korpan Ya.V. Kompleks metodiv i zasobiv zakhystu informatsii u kompiuternykh systemakh / Ya.V. Korpan // Reiestratsiia, zberihannia i obrobka danykh. – 2015. – Vыp. 1. – T. 3 2. – S. 31–35.

7. Lokaziuk V. M. Zasady system pidtrymky pryiniattia rishen na osnovi kompiuternykh system ta yikh komponentiv : navch. posib. / V. M. Lokaziuk, O. V. Ivanov, V. Yu. Titova ; Khmelnyts. nats. un-t. – Khmelnytskyi : Honta A.S., 2010. – 338 c.

Рецензія/Peer review : 25.5.2020 р. Надрукована/Printed : 16.6.2020 р.
Стаття рецензована редакційною колегією