DOI 10.31891/2307-5732-2019-273-3-164-167
УДК 004.38

В.Ю. ТІТОВА, С.О. САВЧУК, В.Ю. ЧЕРНИШ
Хмельницький національний університет

КОНЦЕПТУАЛЬНА МОДЕЛЬ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В СУЧАСНИХ КОМП'ЮТЕРНИХ СИСТЕМАХ

В даній статті проведено деталізацію задач, які виникають під час захисту інформації у комп'ютерних системах від дії шкідливого програмного забезпечення. Після деталізації задачі розмежовано між підсистемами системи захисту інформації, що дозволило спроектувати структуру зазначеної системи. Запропонована авторами структура за рахунок введення у неї інтелектуальних компонентів дозволяє підвищити ефективність захисту інформації в сучасних комп'ютерах.

Ключові слова: концептуальна модель, структурна схема, захист інформації, комп'ютерні системи.

VERA YURIIVNA TITOVA, SERHII OLEHOVYCH SAVCHUK, VLADYSLAV YURIIOVYCH CHERNYSH
Khmelnytskyi National University

CONCEPTUAL MODEL OF THE SYSTEM OF INFORMATION PROTECTION IN MODERN COMPUTER SYSTEMS

The details of tasks that arise during the protection of information in computer systems from the action of malicious software are analysed in this article. Detailing tasks are delimited between the subsystems of the information protection system, which allowed designing the structure of this system. The system of computer information protection consists of the following components: the dialog subsystem, the monitoring subsystem, the planning of inspections subsystem, the update subsystem. The proposed structure doesn't contradict to the "Concept of information security protection in computer systems" adopted to date and takes into account the measures taken to automate the protection of information in modern computer systems. It also can improve the effectiveness of information security in modern computers by introducing its intellectual components.

Keywords: *conceptual model, structure diagram, information protection, computer systems.*

Вступ

В сучасному суспільстві комп'ютерні системи активно впроваджуються у фінансові, юридичні, промислові, торгові та соціальні галузі. У зв'язку з цим швидко зростає інтерес до проблем збереження та захисту інформації.

Тривалий час методи захисту інформації розроблялися тільки державними органами, а їхнє впровадження розглядалося як виняткове право певної держави [1–3]. Проте в останні роки збільшилися спроби несанкціонованого доступу до конфіденційної інформації, а проблеми захисту інформації виявилися в центрі уваги багатьох вчених і спеціалістів різних країн.

Згідно з оглядами міжнародних агентств з інформаційної безпеки, можна констатувати таке [3]:

- метою створення шкідливих програм і проведення атак стає, крім отримання грошового прибутку, крадіжка і подальше використання будь-якої можливої інформації
- з'являється новий клас шкідливих програм, націлений як на крадіжку персональної інформації користувачів, так і на тотальну крадіжку всіх інших даних.

А тому однією з актуальних на сьогоднішній день задач є вирішення питань ефективного захисту інформації, як від зовнішніх, так і від внутрішніх загроз, за рахунок створення та впровадження систем захисту інформації в автоматизованих системах підприємств, установ та організацій [3].

Характеристика предметної області

На сьогоднішній день існує багато методів та принципів захисту інформації у комп'ютерних системах, серед яких можна виділити групу методи виявлення ШПЗ. Методи даної групи умовно можна розділити на [4–6]:

- сигнатурні або точні методи виявлення шкідливого програмного забезпечення (ШПЗ), засновані на порівнянні вмісту підозрілих програм та файлів з відомими зразками шкідливих програм;
- евристичні або наближені методи, які дозволяють з певною імовірністю припустити, що деяка програма або файл являють собою ШПЗ.

Сигнатурний аналіз полягає у виявленні характерних ідентифікуючих рис кожного ШПЗ і пошуку його шляхом порівняння файлів з виявленими рисами. Сигнатурою ШПЗ вважається сукупність рис, що дозволяють однозначно ідентифікувати наявність його присутність у файлі (включаючи випадки, коли файл цілком є такою програмою). Всі разом сигнатури відомих шкідливих програм складають базу даних ШПЗ. Завдання виділення сигнатур, як правило, вирішують люди-експерти в області захисту комп'ютерної інформації або спеціальні автоматизовані засоби виділення сигнатур [4, 6].

Якщо сигнатурний метод заснований на виділенні характерних ознак ШПЗ і пошуку цих ознак у файлах, то евристичний аналіз ґрунтується на припущенні, що нові шкідливі програми часто виявляються схожі на будь-які з уже відомих та намагаються нанести шкоду комп'ютерній системі. А тому, крім пошуку у файлах вже знайомих сигнатур, даний метод заснований на виділенні основних шкідливих дій, таких як, наприклад: видалення файлу, запис у файл, запис в певні області системного реєстру, відкриття порту на прослуховування, перехоплення даних що вводяться з клавіатури, розсилка листів та ін. [4, 6].

Позитивним ефектом від використання цього методу є можливість виявити нове ШПЗ ще до того, як для нього будуть виділені сигнатури. Негативним – імовірність помилково визначити наявність у файлі шкідливу програму, коли насправді файл її не містить.

Практично, на сьогоднішній день, будь-яка система для захисту комп'ютерної інформації використовує обидва методи виявлення ШПЗ [4–6]. Проте аналіз ефективності таких програм дозволяє зробити висновок, що зазначених методів для успішної роботи недостатньо. Більш того, одне тільки їх використання, зокрема через можливість помилкового спрацьовування, може призвести до великих втрат інформації, а це є неприпустимим.

Постановка задачі

Отже, можна зробити висновок, що для збільшення ефективності захисту комп'ютерної інформації, зазначені системи мають базуватися не тільки на методах виявлення ШПЗ, але й містити допоміжні модулі, які будуть виконувати додаткові задачі.

Концептуальна модель системи захисту комп'ютерної інформації

Серед множини задач, які виникають під час захисту комп'ютерної інформації та виявлення ШПЗ, можна виділити наступні [4–6]:

- задача своєчасного оновлення сигнатурних баз даних;
- задача захисту від можливої втрати інформації у результаті помилкового спрацьовування;
- задача моніторингу присутності ШПЗ в режимі реального часу або згідно з розкладом перевірок.

Оновлення сигнатурних баз може проводитись двома шляхами. Перший – це завантаження з Інтернет-баз останніх версій відомих сигнатур ШПЗ. Другий – це виявлення підозрілих програм та файлів на основі аналізу їх поведінки та внесення їх сигнатур до бази даних після того, як їх шкідлива дія буде підтверджена користувачем.

Захист від помилкового спрацьовування полягає у використанні спеціальних технологій, які дозволяють ізолювати та зберегти підозрілу програму або файл з можливістю їх відновлення користувачем у разі потреби. У більшості сучасних систем захисту інформації такі технології носять назву «карантин».

Задача моніторингу присутності ШПЗ полягає у періодичній перевірці комп'ютерної системи на наявність зазначених шкідливих програм. Дана перевірка може проходити безперервно, в режимі «онлайн», що забезпечує більш ефективний захист, проте потребує більших ресурсних затрат комп'ютерної системи, що може сказатися на її продуктивності в цілому. Або дана перевірка може проводитися за розкладом, який задається користувачем. Це дозволяє знизити використання ресурсів комп'ютерної системи, проте підвищує ризик втрати інформації, оскільки ШПЗ може проникнути у систему між перевірками та встигнути нанести їй шкоду.

Альтернативою цим двом методам є «інтелектуальний моніторинг», який полягає в аналізі діяльності користувача та зміни розкладу перевірок в залежності від неї. Наприклад, якщо користувач активно працює в мережі Інтернет й імовірність проникнення у комп'ютер ШПЗ зростає, система переходить в режим онлайн-моніторингу. А у випадку виконання комп'ютером роботи, непов'язаної з надходженням нових потоків даних, здійснює перевірку щодня або щотижня.

Отже, на основі задач, які має виконувати система захисту інформації було побудовано її концептуальну модель (рис. 1). У овалах зазначені задачі, що покладені на систему. Стрілки вказують напрямки надання інформації та її зміст.

З аналізу наведеної концептуальної моделі можна зробити висновок, що система захисту комп'ютерної інформації має складатися з наступних підсистем: діалогової, моніторингу ШПЗ, планування перевірок, оновлення.

Структура зазначеної системи наведена на рис. 2.

Діалогова підсистема являє собою інтерфейс користувача для зручності спілкування із системою. За її допомогою здійснюється виконання таких функцій, як налаштування параметрів моніторингу ШПЗ, налаштування завантаження оновлень, підтвердження або відхилення додавання до бази нових сигнатур, налаштування графіку перевірок, підтвердження або відхилення видалення підозрілих програм та файлів, які знаходяться у карантині. Крім того, за допомогою цієї підсистеми здійснюється захист налаштувань від зміни їх ШПЗ та забезпечується можливість віддаленого доступу до системи захисту комп'ютерної інформації.

Підсистема оновлення здійснює наповнення бази даних сигнатур відомими сигнатурами ШПЗ з мережі Інтернет та за рахунок пошуку сигнатур підозрілих програм та файлів, шкідлива дія яких підтверджується. Для виявлення зазначених програм та файлів використовуються компоненти штучного інтелекту, а саме система нечіткого логічного висновку, що базується на ознаках діяльності підозрілих програм та файлів, виділених системою моніторингу, та визначає імовірність їх відношення до ШПЗ.

Підсистема планування перевірок базується на графіку перевірок, який задається користувачем, та аналізі діяльності користувача, який дозволяє, за потреби, вносити зміни в зазначений графік. Аналіз здійснюється за допомогою вбудованих систем моніторингу діяльності користувача операційних систем сучасних комп'ютерів.

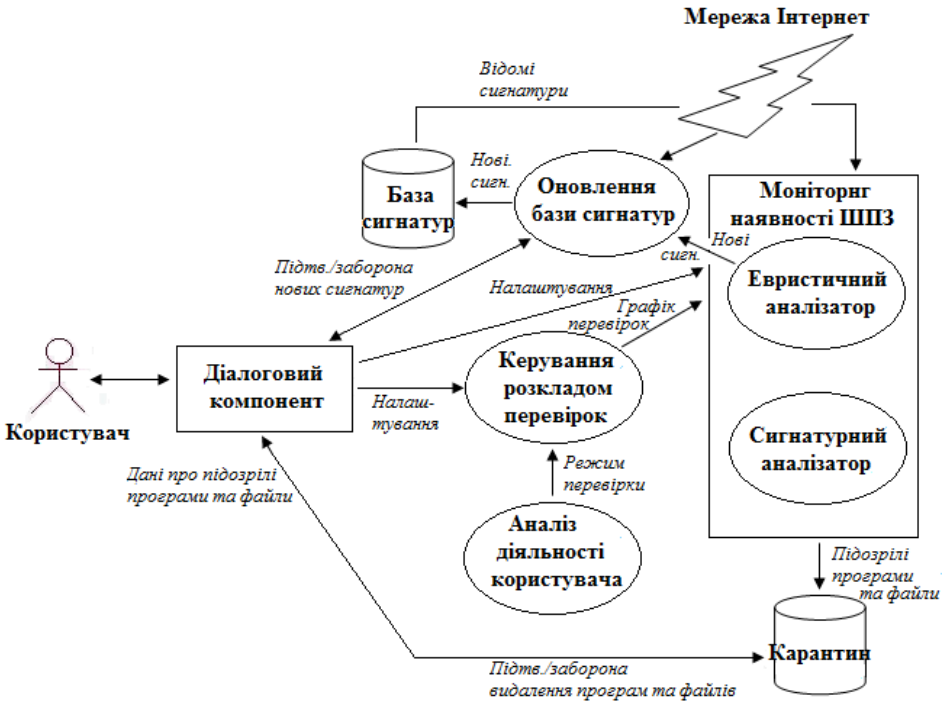

Рис. 1. Концептуальна модель системи захисту комп'ютерної інформації

Підсистема моніторингу ШПЗ базується на відомих на сьогоднішній день методах виявлення шкідливих програм та файлів, а саме сигнатурному та евристичному. Відомі сигнатури ШПЗ необхідні для ефективного моніторингу, надходять з бази сигнатур, яка регулярно оновлюється підсистемою оновлення.

База карантину містить у собі програми та файли, визнані підсистемою моніторингу підозрілими та ізольованими до рішення користувача.

Запропонована система захисту інформації не суперечить прийнятій на сьогоднішній день «Концепції захисту інформації в комп'ютерних системах» [3] та враховує міри, які приймаються з автоматизації захисту інформації в сучасних комп'ютерних системах.

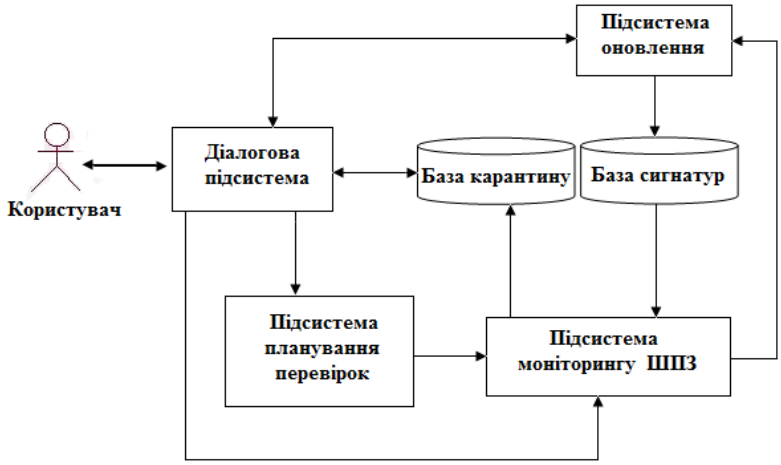

Рис. 2. Структура системи захисту комп'ютерної інформації

Висновки

Підвищення ефективності захисту інформації було досягнуто за рахунок деталізації та розмежування задач, які постають у процесі захисту інформації та виявлення ШПЗ в сучасних комп'ютерних системах, а саме:

- аналізу діяльності користувача та внесення залежно від його результатів коригувань у графік перевірок, заданий користувачем;
- інтелектуального аналізу підозрілих програм та файлів та доповнення за рахунок цього бази даних сигнатур відомого ШПЗ.

Запропоновані на основі проведеної деталізації концептуальна модель та структурна схема є основою для подальшого створення системи захисту комп'ютерної інформації у автоматизованих системах підприємств, установ та організацій.

Література

1. Про державну таємницю [Електрон. ресурс] : закон України // Відомості Верховної Ради (ВВР). – 1994. – № 16, ст. 93. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/3855-12

2. Про Національну систему конфіденційного зв'язку [Електрон. ресурс] : закон України, зі змінами. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/2919-14

3. Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности: стандарт третьего поколения / Ю.А. Родичев. – СПб : Питер, 2018. – 254 с. – ISBN: 978-5-4461-0861-9

4. 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

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

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

References

1. Pro derzhavnu taiemnytsiu [Elektron. resurs] : zakon Ukrainy // Vidomosti Verkhovnoi Rady (VVR). – 1994. – № 16, st. 93. – Rezhym dostupu : http://zakon2.rada.gov.ua/laws/show/3855-12

2. Pro Natsionalnu systemu konfidentsiinoho zviazku [Elektron. resurs] : zakon Ukrainy, zi zminamy. – Rezhym dostupu : http://zakon2.rada.gov.ua/laws/show/2919-14

3. Rodichev Yu.A. Normativnaya baza i standarty v oblasti informacionnoj bezopasnosti: standart tretego pokoleniya / Yu.A. Rodichev. – SPb : Piter, 2018. – 254 s. – ISBN: 978-5-4461-0861-9

4. 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

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

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

Рецензія/Peer review : 26.5.2019 р. Надрукована/Printed : 2.6.2019 р.
Рецензент: д.т.н., проф. Говорущенко Т.О.