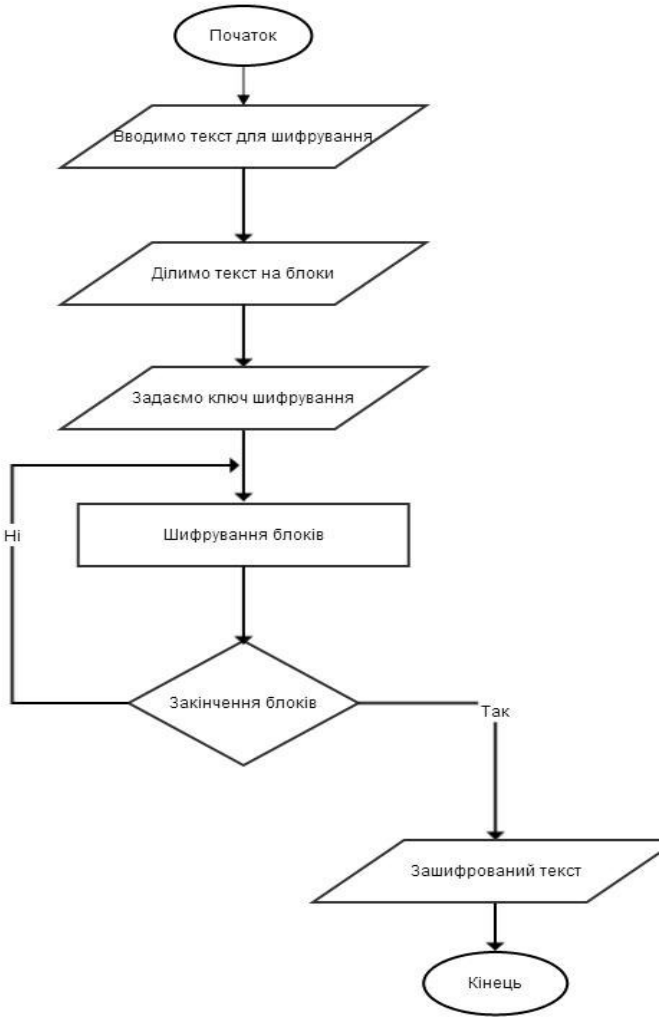

Рисунок 1 - Алгоритм шифрування повідомлень

Список використаних джерел

1. Брюс Шнайер. Прикладная криптография. – М.: Мир, 2005. –с.1204.
2. C-K. Yuen. Testing random number generators by Walsh transform. IEEE Trans. Computers,26(4):329–333, 1977.
3. Тоффоли Т., Марголус Н. «Машины клеточных автоматов» – М.: Мир 1991. –с.728.

УДК 004.056.5

ЗАСТОСУВАННЯ МЕТОДІВ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ У ВИСОКОНАВАНТАЖЕНИХ СИСТЕМАХ

Мєтєлєва Л.В.
Національний технічний університет України «Київський політехнічний інститут», студент

І. Постановка проблеми

Класифікація шкідливого програмного забезпечення та виявлення аномалій у бінарних файлах у високонавантажених системах має свої особливості порівняно з іншими комп’ютерними системами. Для високонавантажених систем є недопустимим виділення значних ресурсів для потокової перевірки виконуваних файлів антивірусом, запуску його у “пісочниці” чи для використання інших методів поведінкового аналізу.

II. Мета роботи

Метою дослідження є розробка швидкого методу класифікації шкідливого програмного забезпечення, застосовного у високонавантажених системах.

III. Методика досліджень

Поширені та відносно ефективні методи поведінкового аналізу (імітації запуску в реальний системи та аналіз поведінки) вимагає значних обчислювальних ресурсів, та не застосовні у випадку високонавантажених систем. Для розв'язання поставленої задачі можна використовувати статистичні методи. Але у даного підходу є суттєві недоліки: необхідно використання значної за обсягом бази сигнатур, яку потрібно постійно оновлювати; не може виявити файли інфіковані новими вірусами. Наступним кроком у цій сфері досліджень є машинне навчання - узагальнена назва штучної генерації знань з досвіду. Штучна система навчається на прикладах і після закінчення фази навчання може узагальнювати. Тобто система не просто порівнює підозрілі дані з відомими зразками, як у статистичних алгоритмів, а розпізнає певні закономірності в даних для навчання.

Найбільш ефективними сучасними алгоритми машинного навчання є J48, J48 Graft, PART, нейронні мережі, SVM та інші.

Крім цього, для підвищення ефективності уже відомих алгоритмів можна використати метод бустингу. Це процедура послідовної побудови композиції алгоритмів машинного навчання, коли кожен наступний алгоритм прагне компенсувати недоліки композиції всіх попередніх алгоритмів.

Зручним Інструментом класифікації у даному дослідженні є набір засобів візуалізації та алгоритмів для аналізу даних і вирішення задач прогнозування - Weka. Weka дозволяє виконувати такі завдання аналізу даних, як підготовку даних (preprocessing), відбір ознак (feature selection), кластеризацію, класифікацію, регресійний аналіз та візуалізацію результатів.

Під час доповіді будуть наведені результати експериментального дослідження ефективності вище загаданих алгоритмів класифікації шкідливого програмного забезпечення.

Висновки

Запропоновано статистичний метод класифікації на основи SVM та методів бустингу для застосування в високонавантажених системах мережевої фільтрації.

Список використаних джерел

1. Sumeet Dua, Xian Du. Data Mining and Machine Learning in Cybersecurity. - Auerbach Pub, 2010. - 240 pp. ISBN-13: 978-1-4398-3942-3
2. Marcus A. Maloof. Machine Learning and Data Mining for Computer Security: Methods and Applications. - Springer Science & Business Media, 2006. - 210 pp. ISBN-13: 978-1846280290

УДК 004.056.53

ЛОКАЛІЗАЦІЯ РАЙДУЖНОЇ ОБОЛОНКИ ОКА ДЛЯ МОБІЛЬНОЇ СИСТЕМИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ЛЮДИНИ

Трифонова К.О.[1)], Гришикашвілі Е.І.[2)], Кілін А.Є.[3)]

Одеський національний політехнічний університет

[1)] ст. викладач; [2,3)] студент

I. Постановка проблеми

В сучасних умовах забезпечення безпеки інформаційних ресурсів представляє собою надзвичайно актуальну задачу. Одною з найпоширеніших процедур обмеження та контролю доступу до інформаційних ресурсів вважається парольна ідентифікація. Яка не зважаючи на важливі переваги, такі як простота реалізації та використання, має значні недоліки завдяки людському фактору: величезна залежність надійності ідентифікації від користувачів, точніше, від обраних ними паролів. У зв'язку з цим та значним підвищенням вимог до інформаційної безпеки набули широкого розповсюдження біометричні методи захисту інформаційних ресурсів. При біометричній ідентифікації використовують унікальні характеристики людини. Метод ідентифікації за райдужною оболонкою ока вважається одним з найбільш точних та надійних способів ідентифікації людини. Першим етапом даного біометричного методу є локалізація, тобто визначення центру зірниці та